FORSCHUNGSZENTRUM JÜLICH GmbH

Zentralinstitut für Angewandte Mathematik

D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

Test von Gigabit-Ethernet-Switches für den Einsatz im JuNet

Dieter Conrads, Olaf Mextorf,

Martin Sczimarowsky, Sabine Werner

FZJ-ZAM-IB-2000-04

Juni 2000

(Letzte Änderung 30.05.2000)

Vorwort

Vor der Einführung von Gigabit-Ethernet-Switching als neue Technik im JuNet wurden durch einen Test geeigneter Komponenten einschlägiger Hersteller die Grundlagen für eine Systementscheidung geschaffen. Bei der Testgeräteauswahl wurden nur solche Hersteller mit nachgewiesener Kompetenz in dem zur Diskussion stehenden Produktbereich berücksichtigt, die mit ihren Produkten bereits im JuNet vertreten waren, um die Betriebs- und Wartungsproblematik im JuNet durch eine weiter vergrößerte Zahl der Partner nicht unnötig zu verschärfen.

Planung und Durchführung der Tests fanden in enger Abstimmung mit dem Zentrallabor für Elektronik (ZEL) statt.

Danken möchten wir an dieser Stelle den Firmen 3Com, Cabletron und Cisco, bzw. den Lieferanten Telonic (3Com), ProData (Cabletron) und Telemation (Cisco) für die Bereitstellung der Geräte und die während der Tests geleistete Unterstützung.

Inhaltsverzeichnis

1 Einleitung

Im Forschungszentrum wurde 1995 mit dem Aufbau eines ATM-Netzes – zunächst im Testbetrieb – begonnen. Auch das B-WiN, an das das Forschungszentrum 1996 über eine 34-Mbps-Leitung angeschlossen wurde, basiert auf ATM-Technik, was die Nutzung dieser Technik auch innerhalb des Forschungszentrums nahelegte. Seinerzeit bestand die Erwartung, daß die universell nutzbare ATM-Technik sowohl im Fernbereich wie im lokalen Bereich allgemeine Verbreitung finden werde.

Seitdem ist der ATM-Technik im lokalen Bereich mit den modernen Ethernet-Varianten (Fast Ethernet (FE, 100 Mbps), Gigabit-Ethernet (GE, 1 Gbps)) auf *Switching*-Basis eine Konkurrenz erwachsen, die zwar funktional unterlegen, dafür aber deutlich billiger ist. Da gleichzeitig neue Dienste, für die die spezifischen ATM-Eigenschaften von besonderem Vorteil sind (insbesondere Multimediadienste), entgegen den Prognosen den Durchbruch zu einer verbreiteten Nutzung nicht geschafft haben, sind die Kostenvorteile der fortgeschrittenen Ethernet-Varianten so gravierend, daß das Forschungszentrum – ebenso wie andere Einrichtungen weltweit auch – dem Rechnung tragen muß.

ZAM und ZEL haben deshalb gemeinsam beschlossen, diese Ethernet-Techniken im JuNet verfügbar zu machen. Die bereits eingeführte ATM-Technik soll dadurch nicht abgelöst werden, sondern den Benutzern sollen wahlweise beide Techniken zur Verfügung stehen. Bei hohen Ansprüchen wie etwa Visualisierungen hoher Qualität (beispielsweise in der Medizin, wo die ATM-Technik ein hohes Maß an Akzeptanz und auch Verbreitung gefunden hat) kann nach wie vor ATM-Technik eingesetzt und ausgebaut werden, wohingegen in Umgebungen, wo im Rahmen der traditionellen Anwendungen Bandbreitenengpässe zu beseitigen sind, in Zukunft eher die leistungsfähigen Ethernet-Varianten zum Einsatz kommen werden.

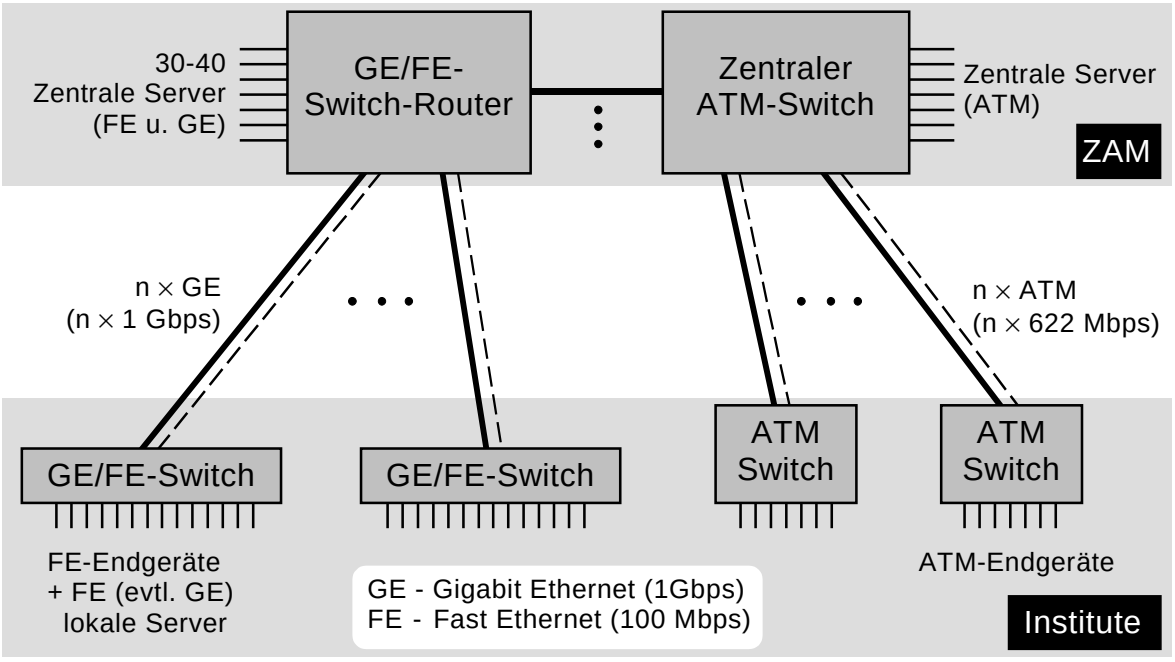

Abb. 1: Zukünftige JuNet-Struktur

Zentraler Punkt eines Gigabit-Ethernet-*Backbone* ist ein groß ausbaubarer *Switch* im ZAM, an den einerseits im ZAM installierte Server und andererseits abgesetzte Gigabit-Ethernet-*Switches* in den Instituten, deren Größe und Ausbau durch die Zahl der anzuschließenden Endgeräte bestimmt ist, angeschlossen werden. Eine Verbindung zwischen dem zentralen ATM-*Switch* und dem zentralen Gigabit-Ethernet-*Switch* verknüpft die beiden Welten, so daß sich die in Abb. 1 gezeigte Grundstruktur ergibt.

Aus heutiger Sicht werden Endgeräteanschlüsse überwiegend in Fast-Eternet-Technik (100 Mbps) erfolgen, wohingegen für Verbindungen zwischen *Switches* und evtl. zu besonders leistungsfähigen Servern Gigabit-Ethernet-Technik (1 Gbps) vorgesehen ist (aus Kapazitäts- und Sicherheitsgründen evtl. auch Mehrfachverbindungen).

Der Einsatz von Ethernet-*Switching* ist ebenso wie der von ATM-Netztechnik an die Existenz einer Sternverkabelung gebunden, so daß nur Gebäude, in denen bereits entsprechende Neuverkabelungsmaßnahmen durchgeführt wurden, dafür in Frage kommen.

2 Vorauswahl von Produkten

Zur Einführung von Gigabit-Ethernet im JuNet war es zunächst notwendig, geeignete aktive Komponenten (*Switches*) auszuwählen. Es bestand von vornherein Einigkeit darüber,

- nur Komponenten eines Herstellers einzusetzen und
- daß dieser Hersteller auch bisher schon mit Produkten im JuNet vertreten sein sollte.

Die Beschränkung auf die Produkte eines Herstellers soll die Wahrscheinlichkeit von Interoperationsproblemen minimieren und darüber hinaus die Möglichkeit offen halten, fortgeschrittene Funktionen (etwa im Bereich der Netzsicherheit) bei Bedarf schon vor der allgemeinen Verfügbarkeit entsprechender standardbasierter Produkte auf der Basis proprietärer Lösungen nutzen zu können.
Die Beschränkung auf einen mit seinen Produkten bereits im JuNet vertretenen Hersteller dient dem Ziel, die Zahl der Partner im JuNet nicht noch weiter zu erhöhen und generell die Betriebs- und Wartungsproblematik nicht unnötig zu verschärfen. Diese Bedingung hatte zur Folge, daß als mögliche Lieferanten nur die Firmen 3Com, Cabletron (als Erbe der Netzprodukte von DEC) und Cisco in Frage kamen.

Zur Herbeiführung einer Systementscheidung wurde mit allen drei potentiellen Herstellern/Lieferanten die Durchführung von Tests vereinbart. Die Vorauswahl der Geräte wurde anhand der verfügbaren Unterlagen vorgenommen. Es sollten jeweils zwei *Switches* von den Herstellern/Lieferanten für die Tests zur Verfügung gestellt werden: ein modular aufgebauter, groß ausbaubarer *Switch*, der als zentraler *Switch* geeignet sein sollte, und ein kleiner, preiswerter *Switch*, wie er in kleineren Instituten zum Einsatz kommen könnte.
Wesentliche Voraussetzungen für die Eignung als zentraler *Switch* waren:

– Ausbaubarkeit (mittelfristig) auf 30-40 FE- und mindestens 50 GE-Anschlüsse
– Redundanz (optional) für alle wichtigen Komponenten.

Da der zentrale *Switch* als *Multilayer Switch* auch *Layer*-3-Funktionalität besitzt, wurde auch die Frage nach IPv6 gestellt. Keines der Geräte unterstützt derzeit IPv6, jedoch

stellen alle Hersteller IPv6-Fähigkeit in Aussicht. Insgesamt wird der IPv6-Fähigkeit seitens der Hersteller derzeit keine besondere Dringlichkeit eingeräumt. Naturgemäß konnten auch keine Angaben über den (finanziellen) Aufwand für eine spätere Nachrüstung gemacht werden. Relativ gut eingrenzbar ist der Aufwand bei Cisco, wo die *Layer*-3-Funktionalität durch ein Aufsteckmodul auf die *Supervisor Engine* realisiert ist, das gegebenenfalls durch ein neues, IPv6-fähiges zu ersetzen wäre. Vom möglichen Aufwand her kritischer ist Cabletron zu sehen, wo die *Layer*-3-Funktionalität auf die einzelnen Interface-Karten verteilt ist.

In den Instituten wird in den kommenden Jahren die Masse der Endgeräte per FE angeschlossen werden. Die eingesetzten *Switches* sollen neben einer den Anforderungen entsprechenden Zahl von FE-Anschlüssen zwei bis drei GE-Anschlüsse bieten: einen als *Uplink* zum zentralen *Switch* im ZAM (zwei, falls Redundanz gewünscht wird) und einen für einen evtl. anzuschließenden leistungsfähigen Server vor Ort.
Auch in Instituten, in denen die Infrastukturvoraussetzungen (Sternverkabelung) erfüllt sind, wird der Übergang auf die neue Technik evolutionär erfolgen, da es, abgesehen von Stellen, wo konkrete Engpässe zu beseitigen sind, meist nicht sinnvoll ist, alte Geräte nachzurüsten, so daß die neue Technik überwiegend im Rahmen von Neubeschaffungen von PCs und Workstations eingeführt werden wird.

Es ist deshalb davon auszugehen, daß zumindest in kleineren Instituten kleine *Switches* für längere Zeit ausreichend sein werden.

Im Laufe der Zeit (und in großen Instituten evtl. sehr bald) kann der Einsatz mehrerer solcher kleinen (*stackable) Switches* (evtl. in Kombination mit einem leistungsfähigen GE-*Switch* zur Verbindung der FE-*Switches* untereinander und mit dem zentralen *Switch*) erforderlich werden.
Wenn sehr viele Anschlüsse zu realisieren sind, kann auch der Einsatz von mittleren oder großen *Switches* sinnvoll sein, da aus Performance- wie aus Effizienzgründen ein leistungsfähiger *Switch* i.a. dem parallelen Einsatz mehrerer kleinerer *Switches* vorzuziehen ist.

Die nachfolgende Beschreibung der *Switches* zeigt, daß auf der Basis der verfügbaren Unterlagen und auch auf der Basis der Preise (für die Preisermittlung wurde eine Einstiegskonfiguration mit 30-40 FE- und 16 GE-Anschlüssen zugrunde gelegt) eine kritischen Nachfragen standhaltende Entscheidung nicht möglich war.

2.1 3Com

Zentraler Switch

Von der Fa. 3Com kommt als zentraler *Switch* das Top-Modell CoreBuilder 9000 in Frage. Hierbei handelt es sich um einen *Multilayer Switch* (*Layer-2-Switching* sowie *Layer-3-Switching* für IP, IPX, Apple Talk) hoher Leistung für Campus-Netze und WAN-Verbindungen (neben FE- und GE-Interfaces stehen auch E3- und T3-Interfaces zur Verfügung; ein 622-Mbps-ATM-Interface ist angekündigt).

Redundanz ist möglich für das *Management&Controller Module*, das *Switching Module*, Netzteile und Lüfter; alle redundanten Module können im laufenden Betrieb ausgetauscht werden.

Als Routing-Protokolle werden OSPF, RIP und RIP-2 unterstützt .

Trunking (bis zu 8 × FE und 6 × GE) ist möglich.

Als Interface Module werden (u.a.) angeboten

- FE bis zu 36 *Ports* (als *Switching Interface Module*)
- GE 9 *Ports* SX (als *Switching Interface Module)*
- GE 2 *Ports* (SX oder LX)
- FE 12-*Ports* TX, *Layer 3 Switching Interface Module*

Beim CoreBuilder 9000 handelt es sich um ein 16-*Slot*-Chassis. Von diesen stehen 14 für Interface-Karten zur Verfügung; zwei sind für redundante *Switching*-Module reserviert; zwei zusätzliche *Slots* sind für redundante *Management&Controller*-Module vorhanden. Der Nachteil der geringeren *Port*-Dichte insbesondere der GE-Interface-Karten (verglichen mit dem Cisco 6500) wird durch die größere Anzahl der Steckplätze wettgemacht.

Das Konzept sieht vor, daß die passive redundante (doppelte Sternverbindungen zu den redundanten *Switch*-Modulen) *Backplane*, deren Kapazität bis 560 Gbps reicht, und das (bzw. die) *Management&Controller*-Modul(e) beim weiteren leistungsmäßigem Ausbau des CoreBuilder 9000 unverändert erhalten bleiben. Das (die) *Switching*-Modul(e) kann (können) im Laufe der geplanten Entwicklung gegen solche höherer Leistung (70 Gbps vollduplex) ausgetauscht werden, sobald sie zur Verfügung stehen, und die Interface-Module gegen solche mit höheren *Port*-Dichten, um die dann verfügbaren Durchsatzleistungen nutzen zu können.

Der CoreBuilder 9000 wird angeboten als

- ATM-*Switch* (mit einem *ATM Switch Module*, welches ATM-Zellen vermittelt) oder
- GE-*Switch* (mit einem *GE-Switching Module*, welches Ethernet-*Frames* vermittelt).

Hier ist die GE-Variante von Interesse. Das derzeit verfügbare *Switching*-Modul erlaubt 24 Vollduplex-GE-Verbindungen (Gesamtdurchsatz 48 Gbps).
3Com verfolgt den Ansatz, das *Layer-3-Switching* auf die Interface-Module zu verteilen, so daß die Leistung mit der Zahl der eingesetzten Interface-Module steigen kann. Bisher stehen allerdings nur FE-*Layer-3-Switching-Interface*-Module zur Verfügung (12 *Ports* TX oder 10 *Ports* FX). Die *Layer*-3-Funktionalität ist nicht auf die Interfaces des Moduls beschränkt. Sie kann als sogenannter *One-armed*-Router von allen *Frames* genutzt werden. Allerdings ist der Durchsatz dann auf die Leistung der Verbindung des *Slots* mit dem *Switching*-Modul (2 Gbps vollduplex) beschränkt, die bei dieser Art der Nutzung im Grunde noch zu halbieren ist, da jeder *Frame* vom *Switching*-Modul zum Router und zurück zu übertragen ist. Unklar ist das Zusammenspiel mehrerer solcher Router, falls mehrere *Layer-3-Switching-Interface*-Module eingesetzt werden. Überdies wird dadurch die Anschlußkapazität für GE reduziert, da die (bisher) nur mit FE-Interfaces bestückten *Layer-3-Switching*-Module *Ports* blockieren, die dann nicht mehr für GE-Anschlüsse zur Verfügung stehen.

Die Interface-Module hoher *Port*-Dichte sind als *Switching-Interface*-Module realisiert, bei denen der Verkehr zwischen den auf dem Modul vorhandenen Anschlüssen durch einen auf dem Modul selbst vorhandenen *Switch* vermittelt wird und nicht zum zentralen *Switching*-Modul weitergeleitet werden muß. Dies ist vor allem für das 9-*Port*-GE-Interface von großer Bedeutung, weil für die 9 Gbps Außenanschlußkapazität ($9 \times$ GE) nur 2 Gbps (jeweils vollduplex) für die Verbindung zwischen Interface-Modul und dem zentralen *Switching*-Modul zur Verfügung stehen. Abgesehen davon, daß es nicht wünschenswert ist, Verkehrsflüsse analysieren zu müssen, um Verbindungen mit hohem Verkehrsaufkommen auf einer Interface-Karte zu vereinen (damit die auf der Interface-Karte vorhandene Vermittlungkapazität optimal genutzt werden kann), wird die freie Zuordnung von Verbindungen durch die starre Auslegung der GE-Anschlüsse als SX-*Ports* (für kurze Entfernungen) behindert. Konsequenterweise hätten die GE-*Ports* als allgemeine *Ports*, die durch GBICs (*Gigabit Interface Converters*) frei an die Gegebenheiten anpaßbar sind, ausgeführt sein sollen.

Die Forderung, am zentralen *Switch* 30-40 FE-Anschlüsse verfügbar zu haben, kann durch ein 36-*Port*-FE-Modul erfüllt werden (ergänzt durch weitere 12 Anschlüsse eines *Layer-3-Switching-Interface*-Moduls). Ein *Slot* muß für ein 622-Mbps-ATM-Modul reserviert werden, so daß 11 Steckplätze für GE bleiben, was eine ausreichende Zahl (die genaue Zahl hängt davon ab, ob 2- oder 9-*Port*-Module verwendet werden (können)) von GE-Anschlüssen ermöglicht (zumal in Zukunft mit weiteren Interface-Modulen hoher *Port*-Dichte zu rechnen ist).

3Com CoreBuilder 9000 (mögliche Startkonfiguration):

16-*Slot*-Chassis	94.870,-
Red. *Power Supply*	9.150,-
36-*Ports* FE (10/100Base-TX)	23.800,-
12-*Ports* 10/100Base-TX *Layer 3 Switching Module*	39.800,-
9-*Ports* 1000Base-SX	35.800,-
8-*Ports* 1000Base-LX (4×2 *Ports* à 15.800)	63.200,-
	DM 266.620,-
abzügl. 50%	DM 133.310,-
	DM 133.310,-

Instituts-Switch

Als kleiner Instituts-*Switch* kann der SuperStack II Switch 3900 dienen.

Gerät mit 36 *Ports* FE(10/100) + 1 *Port* 1000Base-SX	23.850,-
1 *Port* 1000Base-LX (Zusatz-*Board*)	5.300,-
	DM 29.150,-
abzügl. 50%	DM 14.575,-
	DM 14.575,-

2.2 Cabletron

Zentraler Switch

Von der Fa. Cabletron kommt als zentraler *Switch* der SmartSwitch Router 8600 (SSR 8600) in Frage. Hierbei handelt es sich um einen *Multilayer Switch* (*Layer-2-Switching* sowie *Layer-3*- und *Layer-4-Switching* für IP und IPX) hoher Leistung für Campus-Netze und WAN-Anbindung (HSSI Interface für E3/T3-Verbindungen ist verfügbar). Ein ATM-Interface (622-Mbps?) ist angekündigt, steht aber noch nicht zur Verfügung.

Redundanz ist möglich für das *Control Module*, Netzteile und Lüfter; alle redundanten Module (auch Interface-Karten) können im laufenden Betrieb ausgetauscht werden.

Die wichtigsten Routing-Protokolle (OSPF, RIP, RIP-2, BGP-4) werden unterstützt .

Trunking (bis zu 4 parallele Verbindungen) ist möglich.

Die Bandbreite der *Backplane* (*Crossbar*) beträgt 32 Gbps (über 30 Mpps).

Der SSR 8600 verfügt über ein 16-*Slot*-Chassis, wovon unter Berücksichtigung von zwei (redundanten) *Control*-Modulen und einem ATM-Interface 13 mit FE- und GE-Interface-Karten bestückt werden können. Da nur Interface-Module mit vergleichsweise geringer *Port*-Dichte angeboten werden (8-fach FE (TX oder FX) und 2-fach GE (SX oder LX)), bleiben bei einem Ausbau mit 40 FE-Anschlüssen 8 *Slots* für GE, d.h. maximal 16 GE-Anschlüsse, d.h. die projektierte Einstiegskonfiguration stellt bereits den Maximalausbau dar. Damit ist dieses Gerät für den Einsatz an zentraler Stelle im Forschungszentrum nicht ausreichend ausbaufähig. Es soll aber in Kürze ein leistungsfähigerer *Switch* mit Interface-Karten höherer *Port*-Dichte angeboten werden, der unseren diesbezüglichen Anforderungen genügen würde.

Positiv hervorzuheben ist die konsequente Auslegung des Gerätes als *Layer-4-Switch*, der auch beim Routen unter Berücksichtigung von *Layer-4*-Informationen (*Flows* auf der Basis von *Port*-Nummern) ohne Geschwindigkeitseinbußen (> 30 Mpps für *Layer-2-, 3-,* und *4-Switching*) arbeitet. *Accounting* und *Access Control Lists* (bis 20.000 Filter) sollen ebenfalls mit Leitungsgeschwindigkeit möglich sein. Bemerkenswert ist die sehr hohe Zahl unterstützter Adressen (800.000 MAC-Adressen auf Ebene 2, 250.000 *Routes* auf Ebene 3 und 4.000.000 *Flows* auf Ebene 4).

Cabletron SmartSwitch Router 8600 (mögliche Startkonfiguration):

16-*Slot* Chassis	9.655,50
2 *Power Supplies* à 2.893,50	5.787,00
Control Module (128 MB Memory)	10.621,50
Router Services (auf PCMCIA-*Card*)	3.859,50
PCMCIA-*Card*	478,50
5 × 8-*Port* FE (TX) à 5.791,50	28.957,50
4 × 2-*Port* GE (SX) à 7.723,50	30.894,00
4 × 2-*Port* GE (LX) à 11.104,50	44.418,00
	DM 139.497,00

Instituts-Switch

Ein sehr preiswerter kleiner Intituts-*Switch* ist der SmartStack 10/100/1000. Als *Layer-2-Switch* mittlerer Größe kommt der SmartSwitch 6000 in Frage.

Cabletron SmartStack 10/100/1000 (4,2 Gpbs *Switching Fabric*, 3,6 Mpps)

Gerät mit 24 *Ports* FE(10/100) + 2 *Ports* GE	3.859,50
1 GPIM LX (*GE Port Interface Module*)	1.637,00
1 GPIM SX	671,50
	DM 6168,00

Für das 2. Hj. 1999 ist eine Variante mit 48 FE-*Ports* (+ 2 GE-*Ports*) angekündigt.

Cabletron SmartSwitch 6000 (modular)

Grundgerät (incl. 500 W Netzteil)	4.086,50
3 × 24 *Ports* FE (TX) à 6757,50	20.272,50
2 *Ports* GE (VHSIM)	1.927,50
2 × GPIM LX à 1637	3.274,00
	DM 29.560,50

2.3 Cisco

Zentraler Switch

Als zentraler *Switch* kommt von der Fa. Cisco der Catalyst 6500 in Frage. Hierbei handelt es sich um einen *Multilayer Switch* (*Layer-2-Switching* sowie *Layer-3-Switching* für IP, IPX, DECnet u.a.) hoher Leistung für Campus-Netze (bisher sind nur FE- und GE-Interfaces verfügbar, für das 2. Hj. 1999 ist ein 622-Mbps-ATM-Interface angekündigt).

Redundanz ist möglich für die *Supervisor Engine*, *Switch Fabric*, Netzteile und Lüfter; alle redundanten Module können im laufenden Betrieb ausgetauscht werden.

Die wichtigsten Routing-Protokolle (OSPF, IGRP, EIGRP, RIP, RIP-2) werden unterstützt.

Trunking (bis zu 8 parallele Verbindungen) ist für FE und GE möglich.

Die Bandbreite der derzeit verfügbaren *Backplane* (*Switching Bus*) beträgt 32 Gbps (16 Gbps vollduplex); das Modell 6500 ist für die Nachrüstung eines 128-Gbps-*Crossbar Switches* (vollduplex) vorbereitet.

Als Interface Module werden (u.a.) angeboten

- 8-*Port* GE
- 16-*Port* GE (2. Hj. 99)
- 48-*Port* FE (10/100)
- 24-*Port* FE (100Base-FX).

Positiv hervorzuheben sind die hohe *Port*-Dichte der verfügbaren Interface-Module, insbesondere der GE-Module, und die Tatsache, daß die GE-*Ports* grundsätzlich als allgemeine *Ports* ausgebildet sind, die durch entsprechende GBICs (*Gigabit Ethernet Inter-*

face Converters) für den gewünschten Einsatzbereich (kleine Entfernung/große Entfernung, *Multimode*/*Single Mode*-LWL) konfektioniert werden.

Das größere der angebotenen Chassis (6509) hat 9 *Slots*, wovon 6 im FZ für die Bestückung mit FE- und GE-Modulen zur Verfügung stehen: Ein *Slot* wird durch die *Supervisor Engine* (SE) belegt, ein weiterer durch das *Layer-3-Switching*-Modul (ab 2. Hj. 99 als Aufsteckmodul für die *Supervisor Engine* lieferbar, wodurch der *Slot* für eine redundante *Supervisor Engine* frei wird und überdies der maximale Durchsatz von 6 Mpps auf 15 Mpps ansteigt), und ein dritter muß für ein ATM-Interface für die Verbindung zum ATM-*Backbone* reserviert werden.

Die Forderung, am zentralen *Switch* 30-40 FE-Anschlüsse verfügbar zu haben, kann durch ein 48-*Port*-FE-Modul erfüllt werden. Es bleiben dann 5 Steckplätze für GE, was bei Verwendung von 16-*Port*-Modulen einen Ausbau auf maximal 80 GE-Anschlüsse erlaubt.

Die derzeit verfügbare *Switch Engine* (Durchsatz 32 Gbps) kann die Anschlußkapazität bei Maximalausbau nicht verlustfrei bewältigen; dies wird erst mit dem angekündigten *Crossbar Switch* möglich sein. Dies ist für die Situation im Forschungszentrum aber kein Nachteil, da anfangs eine kleine Ausbaustufe ausreicht und überdies nicht damit zu rechnen ist, daß sofort auf allen etablierten Anschlüssen gleichzeitig mit maximaler Rate übertragen wird. Die Strategie von Cisco (bereits heute in summa noch nicht voll nutzbare Interface-Karten hoher *Port*-Dichte verfügbar zu machen) hat den großen Vorteil, daß – um die zukünftig verfügbaren (und dann wahrscheinlich auch benötigten) hohen Vermittlungskapazitäten nutzen zu können – nicht notwendig neue Interface-Karten beschafft werden müssen.

In der letzten Ausbaustufe ist die Verteilung der *Layer-3-Switching*-Funktionalität, d.h. die Verlagerung in die Interface-Module, vorgesehen. Hier ist zu klären, wie mehrere solcher *Layer*-3-fähiger Interface-Karten untereinander und mit der auf der *Supervisor Engine* verfügbaren *Layer*-3-Funktion zusammenarbeiten. Außerdem könnte die Nutzung der verteilten *Layer*-3-Funtionalität (falls nicht durch Aufsteckmodule realisiert) bedeuten, daß die bis dahin vorhandenen Interface-Module ausgetauscht werden müßten (falls sehr hohe *Layer-3-Switching*-Kapazitäten benötigt werden).

Cisco Catalyst 6509 (mögliche Startkonfiguration)

Grundgerät	13.059,10
Power Supply	5.700,00
Red. Power Supply	5.700,00
Supervisor Engine	13.059,10
Layer-3-Module	26.126,80
48-*Port* FE (10/100)	16.980,70
16-*Port* GE	23.514,55
8 × GBIC LX/LH (à 1.960,80 DM)	15.686,40
8 × GBIC SX (à 653,60 DM)	5.228,80
RMON-Lizenz	3.000,00
	DM 128.055,45

Instituts-Switch

Als kleiner Instituts-*Switch* ist der Catalyst 2948 geeignet. Ein Beispiel für einen flexibel ausbaubaren *Switch* mittlerer Leistung mit günstigen *Port*-Kosten ist der Cisco Catalyst 4000.

Cisco Catalyst 2948 (fixed)

Gerät mit 48 *Ports* FE(10/100) + 2 *Ports* GE	10.272,70
1 GBIC LX/LH	1.960,80
1 GBIC SX	653,60
	DM 12.887,10

Cisco Catalyst 4003 (modular)

Grundgerät (incl. *Supervisor Engine*)	10.446,95
32-*Ports* FE (10/100) + 2 *Ports* GE	5.873,80
2 GBIC LX/LH	3.921,60
48-*Ports* FE (10/100)	6.257,40
RMON-Lizenz	1.000,00
	DM 27.769,75

3 Technik

3.1 Gigabit Ethernet

Gigabit Ethernet für Glasfaserübertragungsmedien wurde nach 2½ Jahren Beratungszeit vom IEEE unter der Kennung 802.3z im Juni 1998 standardisiert. Ein entsprechender Standard für 4-paariges Kat.-5-Kupferkabel mit 100 m *Link*-Entfernung mit der Bezeichnung 802.3ab folgte Mitte 1999. Der zeitliche Abstand der Standardisierung ist, vor dem Hintergrund der Übertragungsschwierigkeiten für entsprechende Frequenzen bzw. Bandbreiten und der notwendigen Weiterentwicklung von Kodierungstechniken gesehen, durchaus verständlich und hat z.Zt. wenig Einfluß auf die Implementierung von Gigabit Ethernet in Produktionsnetzen, da Gigabit Ethernet hier im wesentlichen als *Backbone*-Technik für *Inter Switch Links* eingesetzt wird und in diesem Bereich ohnehin Glasfaserkabel dominieren.

Sollten in Zukunft leistungsfähige Desktopsysteme und entsprechende Applikationen Gigabit Ethernet bis hin zum Endanwender notwendig werden lassen, so dürfte die Nachfrage nach 802.3ab-Lösungen deutlich steigen.

Der IEEE 802.3z Standard kennt drei *Physical Layer Interfaces* (PHY):

– 1000BaseSX für *Multimode*-Glasfasern (550 m Reichweite, 830 nm Wellenlänge)

– 1000BaseLX für *Single-Mode*-Glasfasern (5 km Reichweite, 1270 nm Wellenlänge) oder für *Multimode*-Glasfasern (550 m Reichweite, 1270 nm Wellenlänge) mit Moden-Anpassungskabel (*Differential Mode Delay*).

– 1000BaseCX für Koaxial- und IBM-Typ-1-Kabel mit 150 Ω Impedanz (25 m Reichweite)

Während für Gigabit Ethernet das Ethernet-*Framing* vom 10-bzw. 100-MBit-Ethernet übernommen wurde, beträgt beim CSMA/CD-Zugriffsverfahren die *Slot Time*, also die Zeit, in der eine Kollisionserkennung stattgefunden haben muß, nicht mehr 512 Bits sondern 512 Bytes. Gleichzeitig wurde es erlaubt, innerhalb der *Slot Time* mehrere Pakete zu übertragen (*burst frames*), um das ansonsten notwendige Auffüllen des Mediums mit nutzdatenfreien *Extension Frames* zu vermeiden. Nur so konnte überhaupt gewährleistet werden, daß mit Gigabit Ethernet im Halbduplex-Mode eine *Collision Domain* von 200 m erreicht werden kann.

Die Verbreitung von Halbduplex-Gigabit-Ethernet-Lösungen ist allerdings sehr gering.

3.2 Switch-Architektur

Bei den *Layer-2-Switches* unterscheidet man in Abhängigkeit von der Ausführung der *Backplane* grundsätzlich zwei Typen.

Bei *Switches* mit einer Ausführung in *Bus*-Architektur sind alle *Ports* eines *Switches* an einem *Bus* angeschlossen. Jedes empfangene Datenpaket muß über den *Bus* zu einer zentralen Stelle (*Supervisor Module, Switch Engine*) gelangen, an der die *Forwarding*-Entscheidung getroffen wird, und anschließend über den *Bus* dann zum Ausgangs-*Port* transportiert werden.

Bei *Switches* mit einer *Backplane* in Matrix-Architektur sind alle *Ports* miteinander vermascht. Die *Forwarding*-Entscheidung wird zwar zentral getroffen, die Pakete können aber auf direktem Weg, mehrere parallel, von ihren Eingangs- zu den Ausgangs-*Ports* transportiert werden, ohne daß gemeinsame Ressourcen aller *Ports* dabei benutzt werden.

Der Vorteil der *Bus*-Architektur liegt in der Möglichkeit, umfangreiche Puffer und eine aufwendige *Forwarding Engine* (mit erweiterten Filter- und Statistikmöglichkeiten) an einer zentralen Stelle effektiv implementieren zu können.

Die Nachteile liegen eindeutig in dem durch die sequentielle Arbeitsweise eines *Bus* prinzipiell eingeschränkten Durchsatz.

Im Gegensatz dazu existiert mit der parallel arbeitenden Matrix-*Backplane* eine Architektur mit höherem Gesamtdurchsatz, die z.Zt. auch noch Spielraum für eine weitere Steigerung des Paketdurchsatzes durch Erhöhung der Taktung bietet.

Der Nachteil eines Matrix-*Switches* besteht allerdings darin, daß, bedingt durch die auf die Eingangs- und Ausgangs-*Ports* verteilten, relativ kleinen Puffer, bei Überlastung an einem Ausgangs-*Port* auch schnell an einem Eingangs-*Port* Pakete nicht mehr angenommen werden können, die u.U. sogar für einen anderen, freien Ausgangs-*Port* bestimmt sind (*Head of the Line Blocking,* Paket-Rückstau am Eingangs-*Port*).

4 Tests

4.1 Ziel

Vor dem Hintergrund der aktuellen Netzwerksituation des Forschungszentrums lag das Hauptaugenmerk dieser Tests nicht auf dem erreichbaren maximalen Durchsatz der *Switches*, sondern auf der Untersuchung der Funktionalität der Geräte.

Erwartet wurde eine schlüssige Produktlinie mit standardbasierenden Konzepten in sinnvoller und gut managebarer Implementierung. Es wurden die verfügbaren Eigenschaften und deren Anwendungsmöglichkeiten sowie die für die Gerätefamilien aufgezeigten und zum Teil schon implementierten Perspektiven (QoS, CoS, *Security*, ACLs) betrachtet.

Die Interoperabilität der Geräte eines Herstellers, aber auch der kleinste gemeinsame Nenner zwischen Geräten verschiedener Hersteller wurden untersucht.

4.2 Testumgebung

4.2.1 Netzwerk-Komponenten

– 3Com:

- CoreBuilder 9000

Abb. 2: 3Com CoreBuilder 9000

Für den Test stand ein 16-*Slot*-Chassis mit einem Netzteil, einer *Enterprise Management Engine* (EME, 3CB9EME), einer Gigabit-Ethernet-*Switch Fabric* (3CB9FG24), einem *Layer-3*-Modul mit 12 Fast-Ethernet-*Ports* und einem Gigabit-Ethernet-*Backplane-Port* (3CB9RF12R), einem 2-*Port* Gigabit-Ethernet-Modul (1000BaseSX, 3CB9LG2MC), einem 10-*Port* 100BaseFX-Modul (3CB9LF10MC) sowie einem 20-*Port* 10/100BaseTX-Modul (3CB9LF20R) zur Verfügung. Das EME lief zu Beginn der Tests mit der *Operational* Software-Version 2.1.0 und der *Boot*-Software-Version V2.0.1, das *Layer*-3-Modul mit der Version 2.2.0. Während der Tests wurden weitere Software-*Upgrades* durchgeführt.

- SuperStack II 3900

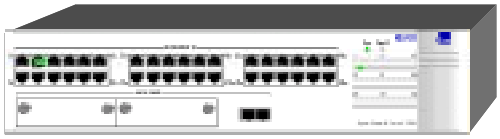

Abb. 3: 3Com SuperStack II 3900

Für den Test stand ein SuperStack II 3900 mit 36 10/100BaseTX-*Ports* sowie einem 1000BaseSX-*Uplink* unter der Software-Version 2.0 zur Verfügung.

- SuperStack II 3300

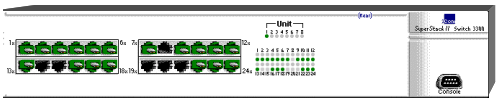

Abb. 4: 3Com Super Stack II 3300

Für den Test stand ein SuperStack II 3300 mit 24 10/100BaseTX-*Ports* unter der Software-Version 2.40 zur Verfügung.

– Cisco:

- Catalyst 6500

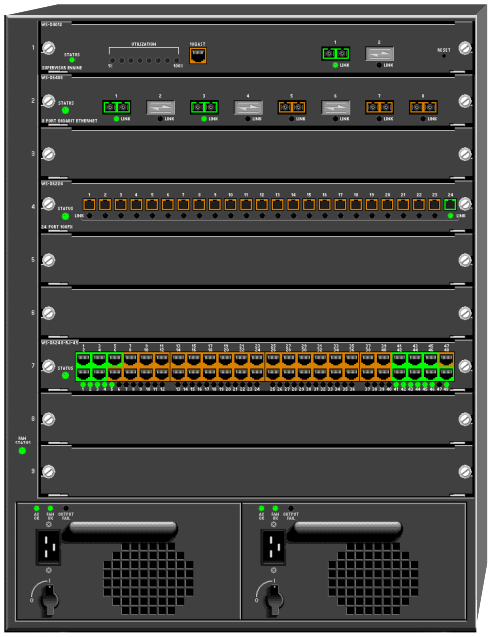

Abb. 5: Cisco Catalyst 6500 Switch

Für den Test stand ein Catalyst 6500 *Switch* mit einem Netzteil, einer *Supervisor Engine* mit zwei Gigabit-Ethernet-*Ports* in Form von GBIC-*Slots*, einem *Multilayer Switch Module* (MSM), einem 8-*Port* Gigbit-Ethernet-Modul (ebenfalls für GBICs), einem 48-*Port* 10/100BaseTX-Modul und einem 24-*Port* 100BaseFX-Modul mit MT-RJ-Konnektoren zur Verfügung.

Das Gerät wurde mit der Software-Version 5.2.1 geliefert und erhielt beim Test ein *Update* auf V5.2.2. Das MSM arbeitete unter IOS 12.0-1a.

- Catalyst 2948G

Abb. 6: Cisco Catalyst 2948G

Für den Test stand ein Catalyst 2948G mit 48 10/100BaseTX-*Ports* und zwei Gigabit-Ethernet-*Ports* in Form von GBIC-*Slots* zur Verfügung. Das Gerät wurde mit der Software-Version 5.2.1 betrieben.

– Cabletron:

- SmartSwitch Router 8600

Abb. 7: Cabletron SSR 8600

Für den Test stand ein SmartSwitch Router 8600 der Fa. Cabletron mit der Software-Version 2.2.0.0, die später auf V2.2.2.0, V2.2.2.2 und auch auf V3.0 Beta 23 aufgerüstet wurde, zur Verfügung. Das 16-*Slot*-Gerät war ausgestattet mit einem Netzteil, zwei *Switching Fabrics*, zwei Kontroll-Modulen SSR-CM2, einem 2-*Port* 1000BaseSX-Modul SSR-GSX11-02, einem 2-*Port* 1000BaseLX-Modul SSR-GLX19-02, einem 8-*Port* 10/100BaseTX-Modul SSR-HTX12-08 und einem 8-*Port* 100BaseFX-Modul SSR-HFX11-08.

- SmartSwitch 2200

  Für den Test stand ein SmartSwitch 2200 mit 24 10/100BaseTX-*Ports* zur Verfügung.

- SmartStack ELS100 24TXG

  Für den Test stand ein SmartStack ELS100 24TXG mit 24 10/100BaseTX-*Ports* unter der Software-Version 2.0.0, die später auf V2.1.0 aufgerüstet wurde, zur Verfügung.

4.2.2 Endgeräte

Neben einigen Netzwerkteilnehmern mit Fast-Ethernet-Anschlüssen fanden folgende Workstations mit Gigabit-Ethernet-Interfaces bei den durchgeführten Tests Verwendung:

– ZAM445:

  DEC Alpha 433au Workstation mit 192 MB Hauptspeicher unter Digital UNIX V4.0E mit Gigabit-Ethernet-Adapter DEGPA 32/64 Bit PCI.

– ZAM050

  DEC Alphastation 500, 333 MHz, mit 128 MB Hauptspeicher unter Digital UNIX V4.0E mit Gigabit-Ethernet-Adapter DEGPA 32/64 Bit PCI.

– ZAM065

  Sun Ultra 60 Modell 1300 mit zwei Ultra-II-Prozessoren 300 MHz, 384 MB Hauptspeicher, Sun Gigabit-Ethernet-Adapter.

– ZAM472

  Sun Ultra 10 mit Ultra-IIi Prozessor 333 MHz unter SunOS 5.7 (Solaris 7), 384 MB Hauptspeicher, Sun Gigabit-Ethernet-Adapter.

4.2.3 Leihstellungen, Firmen, Unterstützung

Die Testkomponenten von 3Com wurden von der Fa. Telonic, Köln, zur Verfügung gestellt. Die Cisco-Komponenten kamen direkt von der Fa. Cisco, Filiale Düsseldorf, und die Komponenten von Cabletron wurden von der Fa. ProData, Grevenbroich, zur Verfügung gestellt.

Nach konkreten Absprachen ca. 2 Monate vor der Teststellung konnte lediglich die Fa. Telonic den zugesagten Liefertermin für die Teststellung einhalten. Die anderen Firmen lieferten mit mehreren Wochen Verspätung.

Während der Testphase standen von allen beteiligten Firmen Ansprechpartner zur Verfügung, bei den Firmen Telonic und ProData konnten die technischen Ansprechpartner jeweils zu zwei Terminen auch vor Ort an den Testgeräten befragt werden.

Aufgrund von Unklarheiten in der *Layer*-3-Implementierung und *Roadmap* des CoreBuilder 9000 konnte von der Fa. Telonic ein Kontakt zum Entwicklerumfeld von 3Com in den USA vermittelt werden.

4.2.4 Durchsatzmessungen

Die Durchsatzmessungen im Bereich *Layer-2-Forwarding* und *Layer-3-Forwarding* wurden wie folgt durchgeführt:

– In jeder Konfiguration wurden mit den beiden oben aufgeführten Sun Workstations *Performance*-Messungen mit dem *Performance-Tool* Netperf, Revision 2.1, das u.a. von Hewlett-Packard entwickelt wurde, gemacht. Die Durchsätze wurden für das TCP-Protokoll gemessen, indem auf jeweils einem System der Netperf-Server gestartet wurde und von dem zweiten beteiligten System mit der Netperf-Client-Software eine Kontrollverbindung zur Übertragung der bei dem Test zu verwen-

denden Parameter wie *Buffer Size*, *Message Size* und Testdauer zum Server aufgebaut wurde. Nach dem Austausch der Kontrolldaten wurde dann der tatsächliche Durchsatztest über eine weitere Verbindung durchgeführt. Bei den Tests wurden die *Socket*-Puffer-Größe (64 - 65536 Bytes) und die Nachrichtenlänge (4 - 65536 Bytes) auf beiden Testsystemen jeweils gleich gegeneinander verändert. Die Messungen wurden mehrfach durchgeführt und die Ergebnisse in einer Graphik aufgetragen.

– In jeder Konfiguration wurden mit den beiden oben aufgeführten DEC Workstations Daten mit dem NFS-Protokoll (TCP-basierend) und dem FTP-Protokoll übertragen. Die Datenübertragung geschah dabei mit 500 MByte großen Testfiles sowohl von Festplatte zum Hauptspeicher ('cp testfile /dev/null') als auch von Festplatte zu Festplatte ('cp testfile1 testfile2'). Bei dem Transfer von Festplatte zu Festplatte wurden weiterhin jeweils lesender (vom NFS-Server zum NFS-Client) und schreibender (vom NFS-Client zum NFS-Server) Zugriff über das Netz untersucht. Beim Test mit dem FTP-Protokoll wurde ebenfalls mit einer 500 MByte großen Datei gearbeitet, die lesend auf '/dev/null' und eine lokale Festplatte sowie schreibend auf die entfernte Festplatte kopiert wurde.

4.3 Testergebnisse

4.3.1 Layer 2

4.3.1.1 Arbeitsweise der Geräte

4.3.1.1.1 3Com CoreBuilder 9000

Der CoreBuilder 9000 arbeitet als modularer *Switch*, bei dem jedes Modul einen eigenständigen *Switch* darstellt (eine Ausnahme stellt hier das Gigabit-Ethernet-Modul dar, das als Verlängerung der *Backplane Ports* zur Front des Gerätes betrachtet werden kann und nicht lokal vermittelt). Die *Backplane* selbst ist, in Form der mittig eingeschobenen *Switch Fabric*, ebenfalls ein Gigabit-Ethernet-*Switch* mit 24 *Ports*. Von diesen *Ports* stehen für die ersten 10 Module je 2 *Ports* als *Backplane Ports* zur Verfügung; die letzten 4 *Slots* des CoreBuilder 9000 bieten den Modulen lediglich einen Gigabit-Ethernet-*Port* zur *Backplane*. Diese Steckplätze bieten sich für die ebenfalls nur über einen Gigabit-Ethernet-*Port* zur *Backplane* verfügenden *Layer*-3-Module an. Dem Vorteil des lokalen, verteilten *Switching* auf den Modulen steht somit ein gewisser Bandbreitenengpaß für modul-überschreitenden Verkehr entgegen. Weiterhin verfügt jedes Modul und auch die *Switch Fabric* über eine eigene Konsole und eine eigene *Bridge*- Konfiguration mit separater *Forwarding Database*.

Die *Spanning-Tree*-Parameter sind bei dem Gerät pro Modul (*Switch*) und pro *Port*, jedoch nicht pro VLAN konfigurierbar. Die Konfiguration einzelner *Ports* zum schnelleren Durchlaufen der *Spanning-Tree-Port*-Zustände im Falle von *Host*-Anschlüssen ist ebenso möglich wie das Setzen von *Broadcast*-Limits pro *Port*. Die Gültigkeitsdauer der *Forwarding-Database*-Einträge ist pro Modul, jedoch nicht pro VLAN einstellbar. Das statische Einfügen oder Entfernen von Einträgen der *Forwarding Database* ist sowohl über die *Command Line* als auch über SNMP möglich; ebenso können MAC-Adressen gesucht werden.

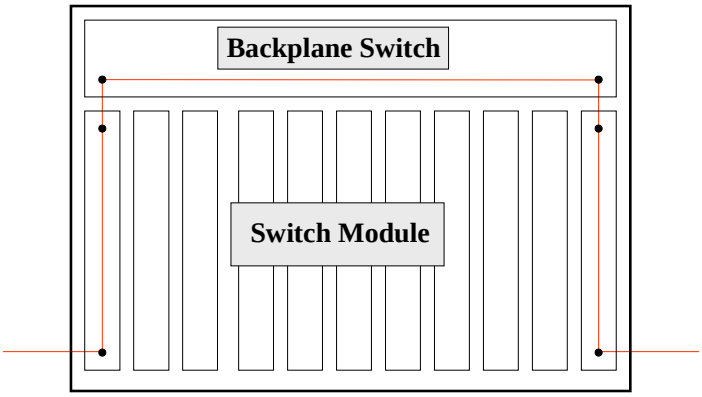

Abb. 8: Modulare Switches im CoreBuilder 9000

Beachtet werden sollte, daß für den gesamten CoreBuilder 9000 die Handhabung der *Forwarding Database* grundsätzlich in zwei sich ausschließenden Modi möglich ist. Im Modus *'all open*' wird pro *Switch*-Modul eine umfassende *Forwarding*-Tabelle für alle VLANs geführt, während im Modus *'all closed'* diese Tabelle separat pro VLAN realisiert wird, allerdings mit deutlichen funktionellen Einschränkungen in einigen Bereichen.

4.3.1.1.2 3Com SuperStack II 3300 und 3900

Die Funktionalität des SuperStack II 3900 ist vergleichbar mit der eines einzelnen CoreBuilder-9000-Moduls. Auch hier wird zwischen den Modi *'all open'* und *'all closed'* unterschieden; die Konfigurationsmöglichkeiten in den Bereichen *Spanning Tree*, *Forwarding Database* und *Broadcast*-Limitierung entsprechen denen des CoreBuilder 9000.

Der *Switch* 3300 arbeitet automatisch mit nur einer *Forwarding Database*. Im Bereich *Spanning Tree* und Management der *Forwarding Database* gilt das für den 3900er Gesagte. Lediglich die *Broadcast*-Limitierung ist hier nicht möglich.

4.3.1.1.3 Cisco Catalyst 6500

Im Gegensatz zum CoreBuilder 9000 arbeitet der Catalyst 6500 mit einer *Bus*-Architektur. Ein lokales *Switching* zwischen den *Ports* eines Moduls ist nicht möglich; es sind jedoch auch keine Module mit einer Einschränkung der Bandbreite zum *Bus* auf 1 Gigabit zu finden. Der gesamte *Switch* wird von einer Konsole aus gesteuert. Da im Catalyst 6500 mit sauber getrennten *Forwarding Databases* pro VLAN gearbeitet wird, sind auch die *Spanning-Tree*-Parameter und das *Aging* pro VLAN (*virtual bridge*) bzw. pro *Port* konfigurierbar. *Broadcast*-Limits sind festlegbar, und eine Manipulation der *Forwarding Databases* (MAC-Adressen eintragen, löschen, suchen) ist über die *Command Line* oder SNMP möglich.

4.3.1.1.4 Cisco Catalyst 2948G

Der Catalyst 2948G wartet mit nahezu den gleichen Möglichkeiten im *Layer*-2-Bereich auf wie der Catalyst 6500. Lediglich das Setzen von *Broadcast*-Limits ist zur Zeit nicht möglich.

4.3.1.1.5 Cabletron SmartSwitch Router 8600

Wie beim CoreBuilder 9000 sind auch beim SSR 8600 die *Spanning-Tree*-Parameter für den gesamten *Switch* bzw. pro *Port*, nicht aber pro VLAN konfigurierbar. Während die Gültigkeitsdauer sogar pro *Port* gesetzt werden kann, konnte keine Möglichkeit gefunden werden, ein *Broadcast*-Limit zu definieren. Aufgrund der Möglichkeit des *Flow Based Switching*, bei dem unter Benutzung von *Layer*-3- und *Layer*-4-Informationen Pakete mit *Wirespeed* weitergeleitet werden können, werden die innerhalb einer *Broadcast*-Domain üblichen Möglichkeiten zum Auslesen und zur Manipulation von *Forwarding Databases* für alle *Ports* des *Switches* noch um Informationen der höheren *Layer* erweitert. Die Tatsache, daß beim Test des 1000BaseLX-Moduls mit einer mehrere Kilometer langen *Single-Mode*-Glasfaserschleife Pakete zwischen zwei Teilnehmern in unterschiedlichen VLANs, die aber über die besagte 1000BaseLX-Schleife zu einer *Broadcast*-Domain verschaltet wurden, nicht weitergeleitet wurden, deutet jedoch auf eine einzige für den gesamten *Switch* geltende *Layer 2 Forwarding Database* hin, die auch Grundlage für das *Flow Based Switching* ist (vergleiche hierzu auch Kapitel 4.3.5 Fehler).

4.3.1.1.6 Cabletron SmartSwitch 2200 und SmartStack ELS100 24TXG

Die Geräte können sowohl als klassische *Bridges* mit allen *Ports* in einer *Broadcast*-Domain als auch als *Switches* mit *Port*-basierenden VLANs betrieben werden. Die üblichen *Spanning-Tree*-Parameter sind pro *Switch* zu konfigurieren. Eine Begrenzung des *Broadcast*-Anteils des Verkehrs war nur beim Betrieb im *Bridge*-Modus möglich. Sobald VLANs betrieben wurden, konnte der *Broadcast*-Anteil nicht mehr begrenzt werden. Eine Umgehung der *Spanning-Tree*-Zustände bis zum *Forwarding* (ca. eine Minute Dauer) für einzelne *Ports* mit *Host*-Anschlüssen schien nicht möglich zu sein.

4.3.1.2 Durchsätze

Getestet wurden die Durchsätze zwischen zwei mit Gigabit Ethernet direkt am jeweiligen *Switch* angeschlossenen Workstations innerhalb eines Subnetzes (VLAN).

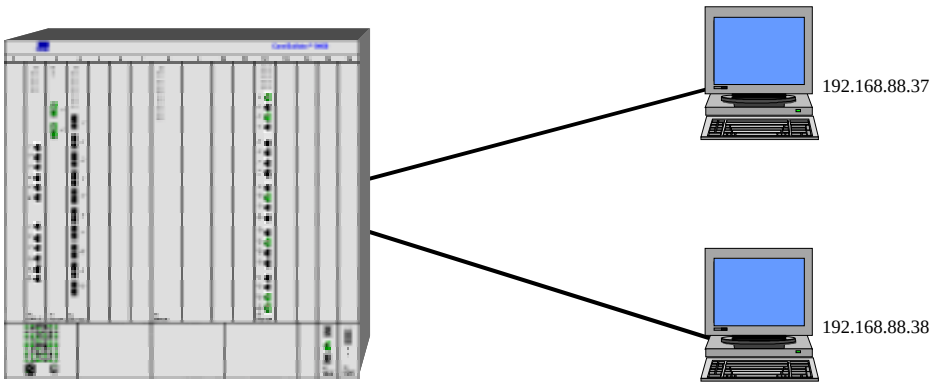

Abb. 9: Testanordnung Layer-2-Switching

4.3.1.2.1 3Com CoreBuilder 9000

Für die *Layer*-2-Durchsatztests wurden die Test-Workstations an jeweils einen *Port* des Gigabit-Ethernet-Moduls angeschlossen und kommunizierten somit lediglich über den 24-Gigabit-*Backplane-Switch*.

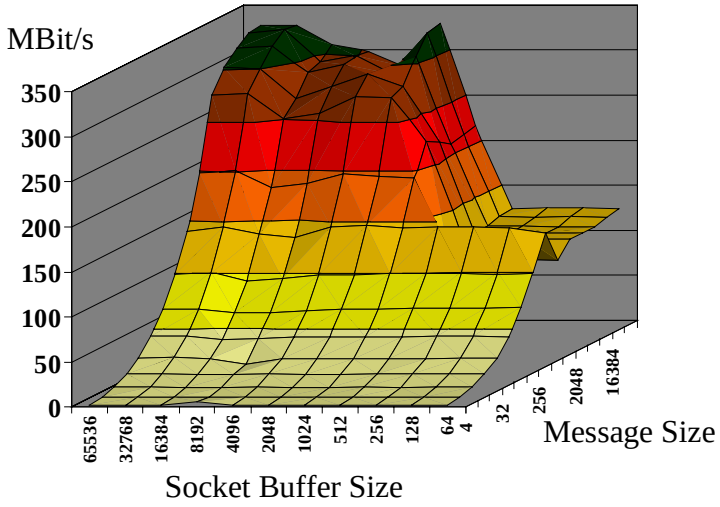

Abb. 10: Ergebnis Netperf Layer 2 mit 3Com CoreBuilder 9000

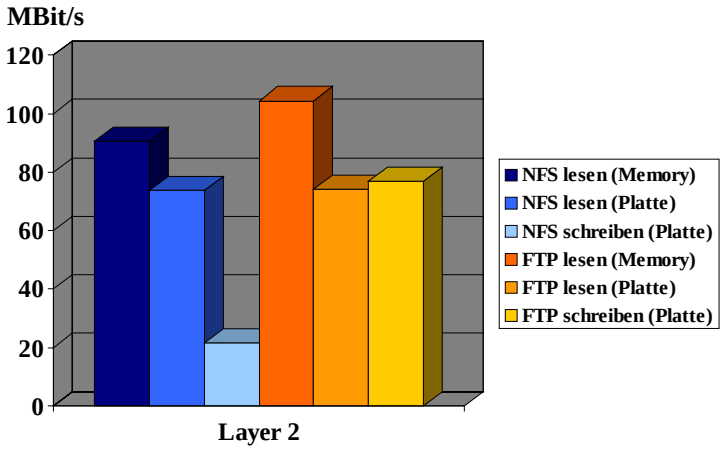

Abb. 11: Ergebnis NFS und FTP Layer 2 mit 3Com CoreBuilder 9000

4.3.1.2.2 Cisco Catalyst 6500

Beim Catalyst 6500 wurden die *Layer*-2-Durchsatztests mit einer Workstation am Gigabit-Ethernet-*Port* der *Supervisor Engine* und einer Workstation an einem *Port* des 8-*Port* Gigabit-Ethernet-Moduls durchgeführt. Da die Module nicht lokal vermitteln, wird der Verkehr in jedem Fall über den *Switch Bus* geführt.

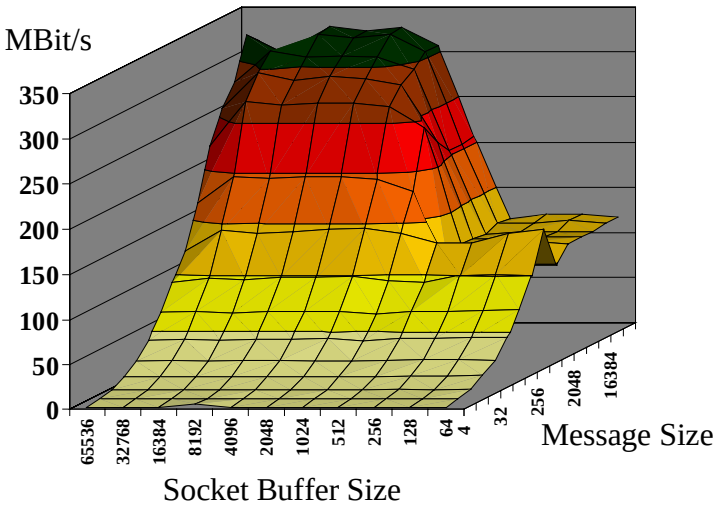

Abb. 12: Ergebnis Netperf Layer 2 mit Cisco Catalyst 6500

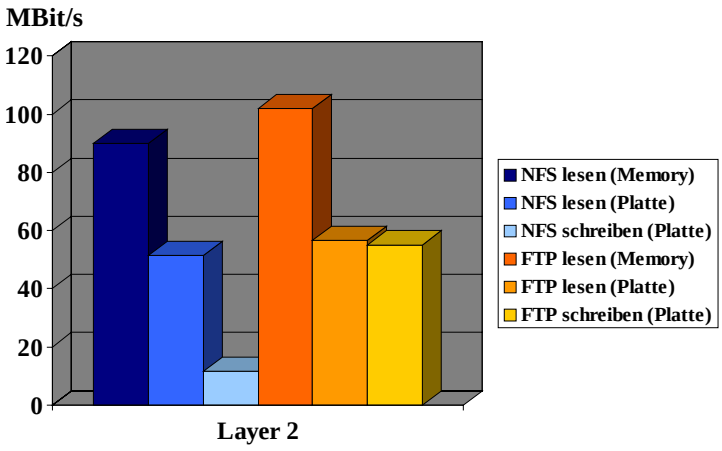

Abb. 13: Ergebnis NFS und FTP Layer 2 mit Cisco Catalyst 6500

4.3.1.2.3 Cabletron SmartSwitch Router 8600

Beim SSR 8600 wurden die Durchsatztests mit Workstations an den beiden *Ports* des 1000BaseSX-Moduls durchgeführt. Die Tests wurden dabei mit und ohne die Option *'flow based switching'* durchgeführt. Die Ergebnisse unterschieden sich jedoch nicht.

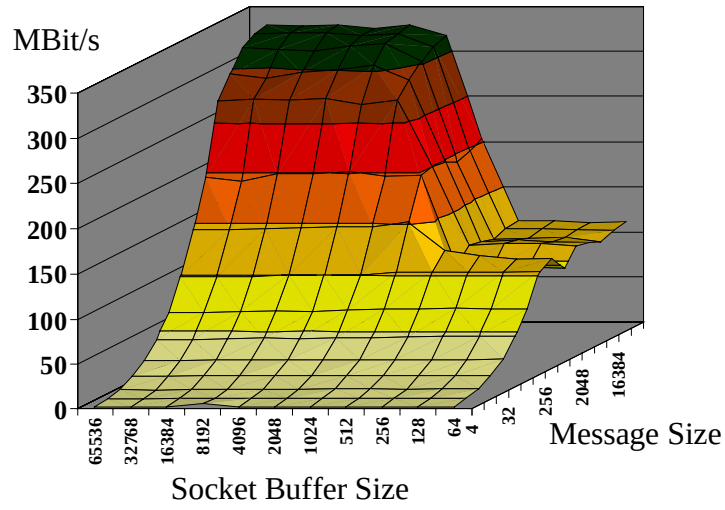

Abb. 14: Ergebnis Netperf Layer 2 mit Cabletron SSR 8600

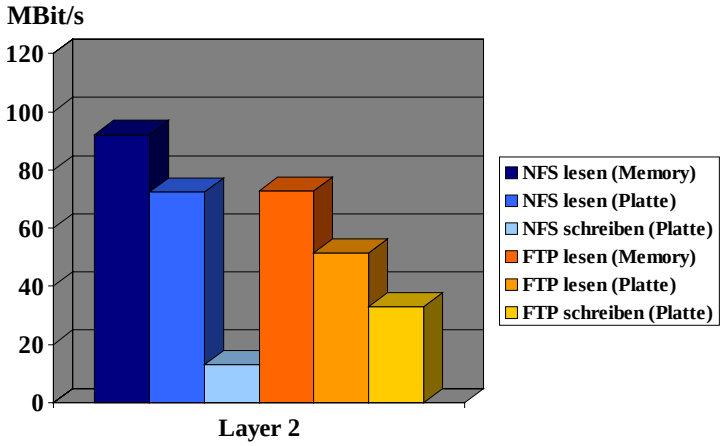

Abb. 15: Ergebnis NFS und FTP Layer 2 mit Cabletron SSR 8600

4.3.1.3 VLANs

Zur Trennung der in einem modernen *Switch* geführten *Broadcast Domains* dienen VLANs, die auch als virtuelle *Switches/Bridges* bezeichnet werden können.

Die Zugehörigkeit eines *Ports* zu einem VLAN kann über vier verschiedene Kriterien festgelegt werden:

– *Port*-basierend:

  Der *Port* wird explizit als zu einem VLAN zugehörig konfiguriert. Alle über diesen *Port* den *Switch* erreichenden Pakete werden ausschließlich in diesem VLAN geführt und weitergeleitet.

– MAC-Adreß-basierend:

  Alle über einen *Port* den *Switch* erreichenden Pakete werden anhand ihrer Absender-MAC-Adresse einem von mehreren VLANs zugeordnet. Vorgegeben wird diese Zuordnung in einer MAC-zu-VLAN Tabelle, die im *Switch* oder aber auf einem externen Server konfiguriert wird.

– Protokoll-basierend:

  Alle über einen *Port* den *Switch* erreichenden Pakete werden anhand des verwendeten Protokolls (IP, IPX, Apple Talk etc.) in entsprechende VLANs sortiert.

– Netzwerk-basierend:

  Alle über einen *Port* den *Switch* erreichenden Pakete werden anhand ihrer Absender-IP-Adresse einem von mehreren VLANs zugeordnet. Vorgegeben wird diese Zuordnung durch die Definition von zu VLANs gehörenden IP-Subnetzen in der *Switch*-Konfiguration.

In der Praxis werden zum größten Teil *Port*-basierende VLANs benutzt. Nur bei ihnen ist durch die feste Zuordnung mit einem Endgerät die versehentliche oder aber absichtliche Zuordnung eines Teilnehmers in ein anderes VLAN aufgrund geänderter IP- oder MAC-Adresse nicht möglich. VLANs sind u.a. auch das Mittel zur Realisierung von Zugriffsrechten und unterschiedlichen Sicherheitszonen in einem Netzwerk. Ihre Grenzen sollten nicht mit geringem Konfigurationsaufwand auf Netzwerkteilnehmerseite absichtlich oder versehentlich durchbrochen werden können.

4.3.1.3.1 3Com

VLAN-Unterstützung beim CoreBuilder 9000:

– *Port*-basierende VLANs sind möglich. Die *Layer*-2-Module unterstützen dabei maximal 127 gleichzeitige VLANs, die *Layer*-3-Module maximal 64 VLANs (in Abhängigkeit von der Zahl der benutzten Protokolle). Nachteilig wirkt sich die Tatsache aus, daß jedes Modul sowie die *Backplane* eigene *Switches* sind und über eine eigene Konsole konfiguriert werden müssen. Beim Einrichten eines Pfades zwischen zwei *Ports* auf verschiedenen Modulen müssen das entsprechende VLAN auf drei Konsolen definiert und insgesamt sechs *Ports* mit ihrer VLAN-Zugehörigkeit konfiguriert werden. Eine Ausnahme bilden hier die 2-*Port* Gigabit-Ethernet-Module, deren Anschlüsse als *Ports* des *Backplane Switches* betrachtet und konfiguriert werden.

– MAC-Adreß-basierende VLANs werden nicht unterstützt.

– Protokoll-basierende VLANs sind, allerdings nur auf Modulen mit *Layer*-3-Funktionalität, nutzbar. Eine weitere Einschränkung ist, daß der *Switch* dazu im *All-Open*-Modus betrieben werden muß. Der *Switch* kann dann jedoch zwischen einer Vielzahl von Protokollen (IP, IPX, Apple Talk, Xerox XNS, DECnet, SNA, Banyan Vines, X.25 und NetBIOS) unterscheiden.

– Netzwerk-basierende VLANs sind, allerdings nur auf Modulen mit *Layer*-3-Funktionalität und ebenfalls im *All-Open*-Modus, konfigurierbar.

VLAN-Unterstützung bei den SuperStack II *Switches* 3300 und 3900:

– Der *Switch* 3900 unterstützt im wesentlichen alle auch auf den *Layer*-2-Modulen des CoreBuilder 9000 möglichen Konfigurationen (und unterliegt auch den gleichen Einschränkungen).

– Auch der *Switch* 3300 bietet im wesentlichen die Möglichkeit, maximal 16 *Port*-basierende VLANs einzurichten. Als etwas einschränkend erweist sich die Randbedingung, daß das Management-IP-Interface des *Switches* immer im VLAN 1 liegt. Außerdem arbeitet der *Switch* 3300 immer mit einer gemeinsamen *Forwarding Database* für alle VLANs (VLAN = *Broadcast*-Container). Außerdem sind für die VLANs neben der üblichen VLAN-ID, die auch beim *Tagging* benutzt wird, auch eine *Local ID* zu vergeben, was gegenüber der bei anderen *Switches* üblichen Praxis des Vergebens von Namen für VLANs ein wenig verwirrt.

4.3.1.3.2 Cisco

VLAN-Unterstützung beim Catalyst 6500:

– *Port*-basierende VLANs sind möglich. Jeder *Port* gehört genau einem von maximal 250 gleichzeitig aktiven bei 1005 möglichen VLANs an.

– MAC-Adreß-basierende VLANs werden nur über einen externen Server unterstützt.

– Protokoll-basierende VLANs werden nicht unterstützt.

– Netzwerk-basierende VLANs werden nicht unterstützt.

VLAN-Unterstützung beim Catalyst 2948G:

– der Catalyst 2948G verfügt im Bereich der VLAN-Konfiguration über die gleichen Möglichkeiten wie der Catalyst 6500, insbesondere ist das Management-VLAN für den *Switch* beliebig definierbar.

4.3.1.3.3 Cabletron

VLAN-Unterstützung beim Cabletron SmartSwitch Router 8600:

– *Port*-basierende VLANs sind möglich. Jeder *Port* gehört genau einem von 4092 konfigurierbaren VLANs an, wobei das VLAN 1 immer vorhanden ist.

– MAC-Adreß-basierende VLANs werden nicht unterstützt.

– Protokoll-basierende VLANs werden unterstützt (als Protokollgruppen werden lediglich IP, IPX und *Bridged Protocols* unterschieden).

– Netzwerk-basierende VLANs werden nicht unterstützt.

VLAN-Unterstützung beim SmartSwitch 2200 und SmartStack ELS100 24TXG:

– Die Unterstützung von VLANs schien bei diesen *Switches* nachträglich implementiert worden zu sein. Die Konfiguration war sehr umständlich, und es mußten beim Betrieb von VLANs einige Einschränkungen in der Funktionalität hingenommen werden.

4.3.1.4 IEEE 802.1Q Tagging

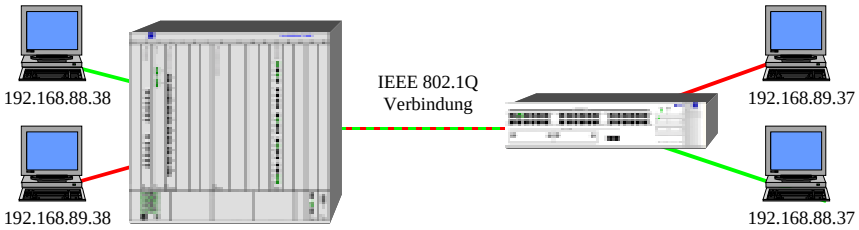

Abb. 16: VLAN-tagging

Um bei geringer Auslastung mehrere VLANs über eine *Inter-Switch*-Verbindung führen zu können und dadurch Ressourcen wie Kabel und *Switch Ports* zu schonen, ist es möglich, Ethernet Pakete nach IEEE 802.1Q mit einer Markierung (*Tag*) zu versehen. Dabei wird gemäß IEEE 802.3ac der Ethernet-*Frame* um 4 Bytes erweitert, von denen 12 Bits das VLAN (1 - 4096) codieren (weitere 3 Bits dienen der Priorisierung nach IEEE 802.1p).

Das Markieren von Paketen nach IEEE 802.1Q wird von allen Herstellern unterstützt. Während Cisco für alle *Switches* und 3Com für den *Switch* 3300 alternativ das entsprechende proprietäre Vorgängerprotokoll (ISL bzw. VLT) mit ähnlicher Funktionalität anbieten, arbeiten die anderen 3Com- und Cabletron-*Switches* lediglich mit 802.1Q-*Tags*.

Während der Tests konnten 802.1Q-Verbindungen zwischen den großen und kleinen *Switches* von 3Com und Cisco geschaltet werden. Lediglich bei den Cabletron-*Switches* konnte ein 802.1Q-*Link* nicht hergestellt werden, da auf den kleinen *Switches* das *Tagging* sehr unlogisch und kaum nachvollziehbar implementiert ist.

Ebenfalls konnten 802.1Q-*Links* zwischen den großen *Switches* der verschiedenen Hersteller konfiguriert und benutzt werden.

Grundsätzlich waren jedoch einige herstellerspezifische Details beim *Tagging* zu beachten:

- Bei 3Com konnte pro *Port* ein VLAN jeweils ohne *Tag* geführt werden. Dazu wurde pro *Port* und dort geführtem VLAN das *Tagging* explizit aus- oder eingeschaltet.
- Bei Cisco konnte das *Tag*-freie VLAN nicht direkt konfiguriert werden. Tatsächlich wird immer das VLAN ohne *Tag* über einen *Link* geführt, dem der *Link Port* vorher *'port-based'* angehörte ('*native* VLAN'). Da dieser Umstand nicht direkt aus der Dokumentation ersichtlich ist, ergaben sich während der ersten 802.1Q-*Link*-Tests einige Stunden Fehlersuche: je nach Historie der beteiligten *Ports* waren einige über den *Link* geführte VLANs nicht nutzbar.
- VTP (VLAN *Trunking Protocol*) konnte nur mit Cisco Komponenten genutzt werden.
- Das VLAN 1 spielt oftmals eine Sonderrolle und wird, abhängig von der *Spanning-Tree*-Implementierung, bei einigen Herstellern zur Weiterleitung der BPDU-*Frames* benutzt. Außerdem wird es bei 3Com teilweise als ein *Fallback*-VLAN für nicht zu VLANs zuordenbare *Frames* benutzt und ist bei den kleinen *Switches* gleichzeitig das Management VLAN (IP-Interface fest im VLAN 1).

4.3.1.5 Trunking

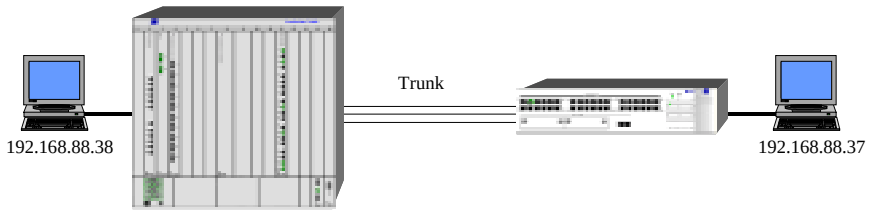

Abb. 17: Trunk zwischen zwei Switches

Trunking (3Com, Cabletron) bzw. *Channeling* (Cisco) bezeichnet die parallele Verwendung von mehreren *Links* zwischen zwei *Switches*.

Aus *Spanning-Tree*-Sicht stellen solche Gruppen von parallelen Verbindungen redundante Pfade dar, die, bis auf einen tatsächlich zu benutzenden Pfad, vom *Spanning-Tree*-Algorithmus automatisch in den *'Blocking'*-Status gesetzt werden.

Beim *Trunking* werden nun die an einem *Trunk* beteiligten *Ports* der *Switches* aus *Spanning-Tree*-Sicht wie ein *Port*-Paar behandelt und nicht blockiert.

Diese *Trunks* stellen eine effektive Möglichkeit dar, die Bandbreite zwischen zwei *Switches* bedarfsorientiert und kostengünstig zu erhöhen, ohne eine neue Übertragungsechnik (z.B. Gigabit Ethernet statt Fast Ethernet) einsetzen zu müssen.

Es ist jedoch darauf hinzuweisen, daß alle Geräte gewisse Einschränkungen bezüglich der Konfiguration der *Trunks* aufweisen:

– 3Com:

  Beim CoreBuilder 9000 können pro Modul bis zu 4 *Trunks* mit maximal je 6 *Ports* (je 8 *Ports* bei den *Layer*-3-Modulen) definiert werden. Empfohlen wird die Aktivierung des proprietären *Trunk Control Message Protocol* (TCMP), das die korrekte Konfiguration und den fehlerfreien Betrieb der *Trunks* kontrolliert. Von den kleinen *Switches* beherrscht lediglich der SuperStack 3900 das TCM-Protokoll. Die am *Trunk* beteiligten *Ports* müssen gleichen Typs und identischer Konfiguration sein. Ein Mischen von Fast- und Gigabit-Ethernet-*Ports* ist nicht möglich. Die Definition eines *Trunks* erlangt erst nach einem Neustart des *Switches* Gültigkeit. Außerdem existiert auch für den *Backplane Switch* eine Beschränkung auf 4 *Trunks*, wobei jedes installierte Gigabit-Ethernet-Modul automatisch als ein *Trunk* zählt. Letztendlich heißt das, daß nicht mehr als 4 Gigabit-Ethernet-Module pro CoreBuilder 9000 eingesetzt werden können. Diese Einschränkung wurde während der Tests durch den Einbau einer aktuelleren Version des *Backplane-Switch*-Moduls auf 6 *Trunks* (Gigabit-Ethernet-Module) gemildert. Als *Workaround* empfiehlt 3Com mehrere Gigabit-Ethernet-Module wiederum zu einem *Trunk* zusammenzufassen, um so mehrere Module pro *Trunk*-Zählung betreiben zu können.

– Cisco:

  Das allgemein als *Trunking* bezeichnete Verfahren zur Zusammenschaltung von *Ports* wird bei Cisco *Channeling* genannt. Beim Catalyst 6500 sind bis zu 128 Channels mit maximal je 16 *Ports* (gleichen Typs) konfigurierbar. Es kann das Cisco-proprietäre *Port Aggregation Protocol* (PagP) benutzt werden, das das Zusammenschalten von *Ports* zu einem *Channel* automatisch durchführen kann.

– Cabletron:

  Cabletron ermöglicht den Aufbau eines *Trunks* wahlweise ohne *Trunking*-Protokoll oder mit dem *Hunt Group Protocol* der Fa. DEC, das u.a. vom DEC Gigaswitch unterstützt wird. Auch bei Cabletron können nur *Ports* gleichen Typs zu einem *Trunk* vereinigt werden.

Weiterhin haben die Geräte von 3Com und Cisco gemein, daß ein solcher *Trunk* zwar aus *Spanning-Tree*-Sicht wie eine Verbindung aussieht, bei der Verkehrsführung jedoch jeder *Trunk Port* weiterhin wie ein *Switch Port* arbeitet, d.h. insbesondere, daß jede *remote* MAC-Adresse über einen dedizierten *Port* eines *Trunks* geführt wird (klassisches *Port*-basierendes *Layer-2-Forwarding*). Eine Vervielfachung des Durchsatzes zwischen zwei *Switches* ist somit nur für mehrere Verbindungen mit unterschiedlichen MAC-Adreß-Paarungen möglich. Der Maximaldurchsatz zwischen einem Endgerätepaar über den *Trunk* ist nicht größer als der über einen einzelnen *Link* des *Trunks* erreichbare Durchsatz. Für Cabletron gilt das obige auf der Basis von *Flows* (*Layer*-3-Adresse und *Layer-4-Port*) statt MAC-Adressen. Entsprechend ist bei unterschiedlichen Anwendungen die Verteilung des Verkehrs zwischen gleichen Teilnehmern über unterschiedliche *Ports* eines *Links* durchaus möglich.

Getestet wurden *Trunks* zwischen den großen und kleinen *Switches* jeweils eines Herstellers. Herstellerübergreifend konnten *Trunks* aufgrund der unterschiedlichen Implementierungen nicht aufgebaut werden.

Alle *Trunks* arbeiteten problemlos. Der Ausfall einer Verbindung innerhalb eines *Trunks* konnte von allen *Switches* selbst bei über diese Verbindung geführtem Verkehr innerhalb weniger Sekunden ausgeglichen werden.

Der maximal erreichbare Durchsatz zwischen 2 Gigabit-Ethernet-Teilnehmern bei dem jeweils getesteten *Trunk* aus mehreren Fast-Ethernet-Verbindungen lag wie erwartet im Bereich von 95 MBit/s, wurde eine zusätzliche Verbindung zwischen weiteren Teilnehmern aufgebaut, so konnte auch diese Verbindung parallel zur ersten mit 95 MBit/s gefahren werden.

4.3.1.6 Priorisierung nach IEEE 802.1p

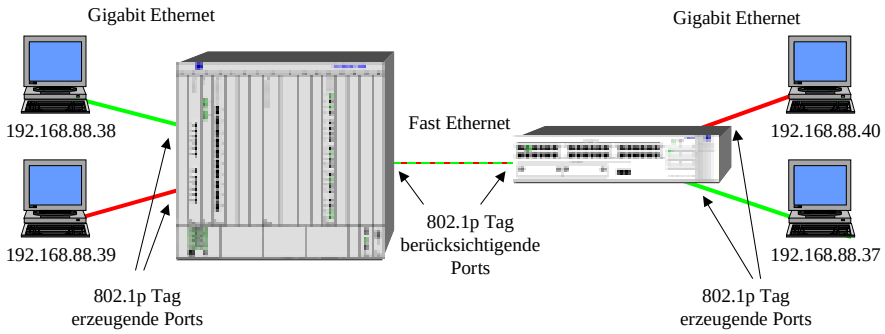

Abb. 18: Testumgebung zur Priorisierung

Um die Weiterleitung von Paketen im Netz mit unterschiedlichen Prioritäten zu ermöglichen und damit die Wahrscheinlichkeit des Verzögerns von zeitkritischen und *'Mission-critical'*-Anwendungen wie z.B. Videodatenströmen oder Verwaltungsdaten durch stark ausgelastete Netzwerk-Ressourcen zu verhindern, können Ethernet-Pakete nach IEEE 802.1p mit 3 zusätzlichen Bits zur Festlegung einer Prioritätsklasse versehen werden. Moderne *Layer-2-Switches* haben idealerweise zwei oder mehr in Hardware realisierte Warteschlangen, die in einem oftmals konfigurierbaren Verhältnis zueinander beim Weitertransport der Pakete berücksichtigt werden und die oft auch bezüglich ihrer Größe unter Berücksichtigung einer vorgegebenen Gesamtgröße aller Warteschlangen konfiguriert werden können. Pakete werden dann entsprechend ihrer Priorität in die Warteschlangen einsortiert.

Da der CoreBuilder 9000 eine Zuordung von Paketen zu Prioritätsklassen und auch die Konfiguration von Warteschlangen und Puffern nur auf den *Layer*-3-Modulen und nur in direkter Verbindung mit RSVP unterstützt, wurden einige kurze Tests zu diesem Thema mit dem Catalyst 6500 und 2948G durchgeführt (Cabletron erlaubt die Definition von Prioritäten für den SSR 8600 durchlaufende *Layer-2- und Layer-3-Flows* anhand der üblichen *Flow*-Parameter (*Ports*, MAC-Adressen, IP-Adressen, TCP/UDP-*Ports*)).

Zu dem Test waren, wie in Abb. 18 zu sehen, an zwei *Switches* je zwei Workstations jeweils über Gigabit Ethernet angeschlossen. Die beiden *Switches* waren lediglich mit Fast Ethernet verbunden. Es kommunizierten immer Workstations an unterschiedlichen *Switches* miteinander.

Wurden keine Einstellungen zur Priorisierung vorgenommen, so erhielten die beiden gleichzeitig laufenden Datenströme ca. 50% der knappen Ressource Bandbreite auf der Fast-Ethernet-Strecke. Bei Netperf-Tests mit großen übertragenen Blöcken ergaben sich Datenraten von 45 bis 52 MBit/s pro Workstationpaar.

Anschließend wurden die Anschluß-*Ports* des ersten Paares kommunizierender Workstations so konfiguriert, daß einkommende Pakete eine hohe Priorität, die des zweiten Paares eine niedrige Priorität bekamen. Die an der Verbindung der beiden *Switches* beteiligten *Ports* wurden so konfiguriert, daß die Priorisierung (802.1p *Tag*) der Pakete bei der Weiterleitung berücksichtigt werden sollte. Es ergaben sich nun bei gleichzeitiger Übertragung Transferraten von 56 bis 74 MBit/s für das erste und 16 bis 32 MBit/s für das zweite Paar.

In einer dritten Anordnung wurde zusätzlich die *Default*-Einstellung für die *Transmit Queue Size Ratio* der Fast-Ethernet-*Ports* von 80 zu 20 (*low priority queue* zu *high priority queue)* auf 20 zu 80 zugunsten des Verkehrs mit hoher Priorität verändert. Die Auswirkungen auf die erreichbaren Transferraten waren sehr deutlich. Das erste Paar konnte mit 93,7 bis 93,9 MBit/s kommunizieren, während sich das zweite Paar mit lediglich 0,1 bis 0,2 MBit/s zufrieden geben mußte.

Wurden die beiden Transfers in dieser dritten Konfiguration nicht gleichzeitig durchgeführt, so erreichte das erste Paar 94,4 MBit/s. Das zweite Paar konnte jedoch auch in dieser Situation, in der die Fast-Ethernet-Verbindung zwischen den *Switches* nicht zwischen zwei Datenströmen geteilt werden mußte, lediglich mit 5,9 MBit/s kommunizieren. Es besteht also das Risiko, daß bei einer allzu restriktiven Konfiguration im Bereich der Empfangs- und Sendewarteschlangen vorhandene Bandbreite nicht genutzt wird und somit künstlich Engpässe erzeugt werden.

4.3.2 Layer 3

4.3.2.1 Router Implementierung

Bei den getesteten Geräten ist die *Layer*-3-Funktionalität (Routing, *Access Control Lists*, Routing-Protokolle, *Accounting* aufgrund von Informationen ab *Layer* 3) lediglich auf den großen *Switches* implementiert. Sie dient hier z.Zt. lediglich dazu, IP-Subnetz-Übergänge in Kombination mit dem *Layer-2-Forwarding* aus einer Hand anzubieten und ist bei den Herstellern 3Com und Cisco z.Zt. diskret in Form eines *Layer*-3-Moduls realisiert. Lediglich der Hersteller Cabletron bietet bereits zukunftsweisend die *Layer*-3-Funktionalität für jeden *Port* im SSR8600 an und arbeitet dabei nach dem *flow-based Switching*-Prinzip, bei dem nach Ermittlung der Verkehrsflußentscheidung aufgrund der TCP-*Port*-, IP-Adreß-, MAC-Adreß- und *Switch-Port*-Informationen die Pakete eines solchen Verkehrsflusses ohne erneutes Durchlaufen des klassischen Route-Prozesses bereits am Eingangs-*Port* erkannt und weitergeleitet werden. Zur besseren Darstellung der Situation zum Testzeitpunkt sollte erwähnt

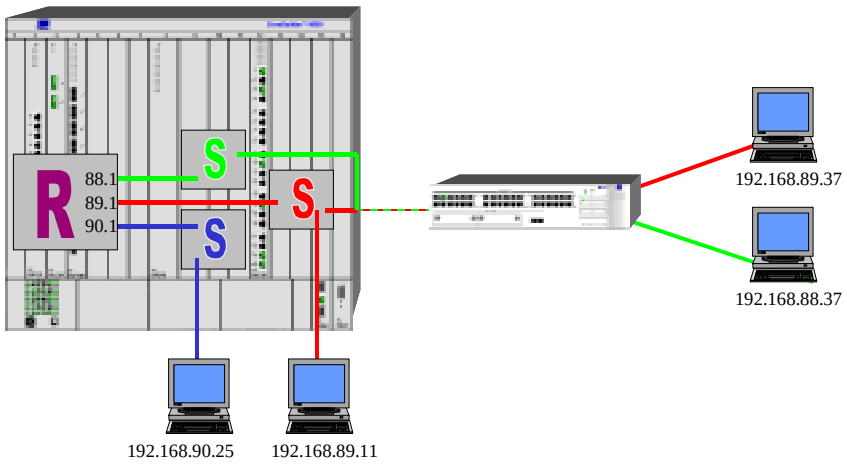

Abb. 19: Routing in einem Layer-2/3 Switch

werden, daß die Fa. Cisco die Routing-Lösung mittels des *Multilayer Switch Modules* (MSM) im Catalyst 6500 eindeutig als Übergangslösung bezeichnet und noch für den Herbst des Jahres 1999 eine Routing-Lösung auf der Basis von zwei Tochter-*Boards* (*Multilayer Switch Feature Card* (MSFC) und Policy *Feature Card* (PFC)) zur *Supervisor Engine* des Catalyst 6500 angekündigt hatte, die als Betriebssystem das von den klassischen Routern bekannte IOS fährt und unter dem Titel *Multilayer Switching* ebenfalls klassische Routing-Entscheidungen innerhalb eines TCP/IP-Datenstromes lediglich einmal zu Beginn trifft und anschließend alle Pakete dieses Datenstromes unter Umgehung der Router-*Engine* klassifiziert und weiterleitet, was zu höheren *Layer*-3-Durchsätzen führt.

Die allgemeine Entwicklung bei den *Switch*-Herstellern geht dahin, *Layer*-3-Funktionalität – und dabei nicht in erster Linie das klassische Routing – auch auf den *Access Switches* verfügbar zu machen. Dazu sind für existierende *Switches* bereits zusätzliche *Boards* bzw. auch neue *Access Switches* in der Entwicklung. Der Sinn dieser Entwicklung liegt zum einen in der Möglichkeit, bereits im Zugangsbereich den von den Teilnehmern empfangenen Verkehr nach verschiedenen Prioritäten klassifizieren und entsprechend weiterleiten zu können (vorteilhaft für stark laufzeitabhängige Dienste wie z.B. Sprachverkehr), aber auch in der Möglichkeit, nach *Layer*-3- und *Layer*-4-Vorgaben Zugriffsregelungen (ACLs) treffen zu können und die Möglichkeit zu haben, *Accounting*-Daten mit *Layer*-3- und *Layer*-4-Information sammeln zu können.

Es folgen einige Details zu den *Layer*-3-Funktionalitäten und Realisierungen der einzelnen Hersteller:

– 3Com:

  Um den CoreBuilder 9000 mit *Layer*-3-Funktionalität auszustatten, muß ein spezielles *Layer*-3-Modul eingeschoben werden, das, wie alle anderen Module und die *Backplane*, praktisch ein eigener *Layer 2/3 Switch* ist, der zur *Backplane* über lediglich einen Gigabit-Ethernet-*Port* und, je nach Ausführung, zur Frontseite z.B. über 12 Fast-Ethernet-*Ports* verfügt. Nur auf den *Layer*-3-Modulen ist die Definition von Protokoll-basierenden und Netzwerk-basierenden VLANs möglich. Pro VLAN läßt das *Layer*-3-Modul die Definiton einer IP-Adresse als Router-Interface zu.

Secondary IP-Adressen werden nicht unterstützt. Diese starke Einschränkung der *Layer*-3-Funktionalität wird sich, wie Anfragen an das Entwicklerumfeld von 3Com in den USA ergaben, auch in Zukunft nicht grundsätzlich ändern. Als *Workaround* zu diesem Problem wurde während der Tests die Möglichkeit des Einsortierens des IP-Verkehrs einer *Broadcast Domain* in mehrere Netzwerk-basierende VLANs mit jeweils zugehörigen Router-Interfaces aufgrund der IP-Absenderadresse ermittelt und getestet. Diese Lösung hat jedoch mehrere gravierende Nachteile: Zum einen ist die Benutzung von Netzwerk-basierenden VLANs nur bei Verwendung des *All-Open*-Modus im gesamten *Switch* möglich, bei dem auf jedem *Switch*-Modul die *Forwarding*-Tabelle für alle VLANs gemeinsam genutzt wird und die damit verbundenen und bereits beschriebenen Probleme auftreten können, und zum anderen ist diese Lösung mit jedem *Layer*-3-Modul nur einmal für eine das Modul über die *Backplane* erreichende *Broadcast Domain* durchführbar, da dem Netzwerk-basierend konfigurierten *Backplane Port* des *Layer*-3-Moduls ein ohne *Tagging* konfigurierter *Port* des *Backplane Switches* gegenüberstehen muß (nur einmal pro *Slot* möglich).

Das *Layer*-3-Modul unterstützt neben den Routing-Protokollen RIP, RIP2 und OSPF, die jedoch nicht getestet wurden, auch die Definition von *Helper*-Adressen zum *Bridging* von *Broadcast*-orientierten Protokollen. Dabei können maximal 32 Kombinationen aus UDP-*Port* und Ziel-IP-Adresse, z.B. für einen Bootp-Server, definiert werden. Filter bzw. *Access*-Listen sind auf dem Modul lediglich in Form von Untergruppen zu VLANs, deren Kommunikation geregelt werden kann, möglich. Hier bleibt das Modul deutlich hinter den Möglichkeiten des CoreBuilders 3500 zurück, auf dessen Hardware es eigentlich basiert. Ohne Studium der CoreBuilder-3500-Beschreibung wäre das Thema *Access*-Listen und Filter der CoreBuilder-9000-Beschreibung komplett unverständlich gewesen. Ein *Tracing* und *Debugging* des Routing-Vorgangs bzw. der Zusammenstellung der *Database* ist beim CoreBuilder 9000 nicht möglich.

– Cisco:

  Um den Catalyst 6500 mit *Layer*-3-Funktionalität auszustatten, bietet Cisco das *Multilayer Switch Module* (MSM) an, das über vier virtuelle *Ports* mit jeweils 1 Gigabit/s Bandbreite mit dem *Switch Bus* kommuniziert. Die Pakete, die über diese 4 *Ports* laufen, können ISL-*Tags* (Cisco proprietär) zur Kennzeichnung der VLAN-Zugehörigkeit enthalten. Ebenfalls können die vier *Ports*, ähnlich wie ein *Channel*, zusammengeschaltet werden, um die vorhandene Bandbreite ins *Layer*-3-Modul effizienter nutzen zu können. Das MSM ist über eine eigene Konsole, zu der von der *Switch*-Konsole aus gewechselt werden kann, zu konfigurieren. Leider unterstützt das Modul nicht das Cisco-eigene VTP-Protokoll, so daß die VLANs auf dem *Layer*-3-Modul neu zu definieren sind. *Secondary* IP-Adressen werden vom Modul ebenso unterstützt wie die Routing-Protokolle RIP, RIP2, OSPF, IGRP und EIGRP. Es können pro Interface mehrere *Helper*-Adressen und auch UDP-*Ports* konfiguriert werden, zu denen entsprechende *Broadcasts* weitergeleitet werden. Filter bzw. *Access*-Listen sind auf dem MSM nicht definierbar. Die *Tracing*- und *Debugging*-Möglichkeiten entsprechen jedoch den auf klassischen Routern unter IOS gewohnten Möglichkeiten.

– Cabletron:

  Der SmartSwitch Router 8600 stellt, wie schon der Name sagt, *Layer*-3-Funktionalität für jeden *Port* zur Verfügung, ohne daß ein zusätzliches Modul oder Tochter-*Board* eingeschoben werden muß. *Secondary* IP-Adressen sind für den SSR 8600 ebensowenig ein Problem wie das *Bridging* einzelner Protokolle über *Helper*-Adressen, bei dem pro IP-Interface und UDP-*Port* eine Ziel-IP-Adresse (Server) angegeben werden kann, zu der entsprechende *Broadcasts* weitergeleitet werden. Die Möglichkeiten zur Definition von Filter- und *Access*-Listen sind sehr umfangreich; so verfügt das System über einen eigenen ACL-Editor in der *Command Line* und erlaubt auch den *Upload* und *Download* von ACL-Files (Definitionen), um diese außerhalb des *Switches* zu editieren. Lediglich das zugehörige *Logging*, das entweder mit einer Ausgabe auf der Konsole des *Switches* oder aber über die *Syslog-Facility* auf einem Server arbeitet, ist nicht optimal ausgelegt. Vor der Ausgabe auf die Konsole wird verständlicherweise bereits in den Unterlagen gewarnt (zu große Datenmengen); die Syslog-Meldungen erreichten in unserem Test nur zu einem kleinen Teil den konfigurierten Server. Außerdem kann nur angegeben werden, daß gar nicht oder aber bei jedem die Filterregeln berührenden Paket ein *Log*-Eintrag erzeugt wird. Der SSR 8600 unterstützt ebenfalls die Routing-Protokolle RIP, RIP2 und OSPF.

4.3.2.2 Durchsätze

Getestet wurden die Durchsätze zwischen zwei direkt an einem *Switch* angeschlossenen Endgeräten in verschiedenen Subnetzen.

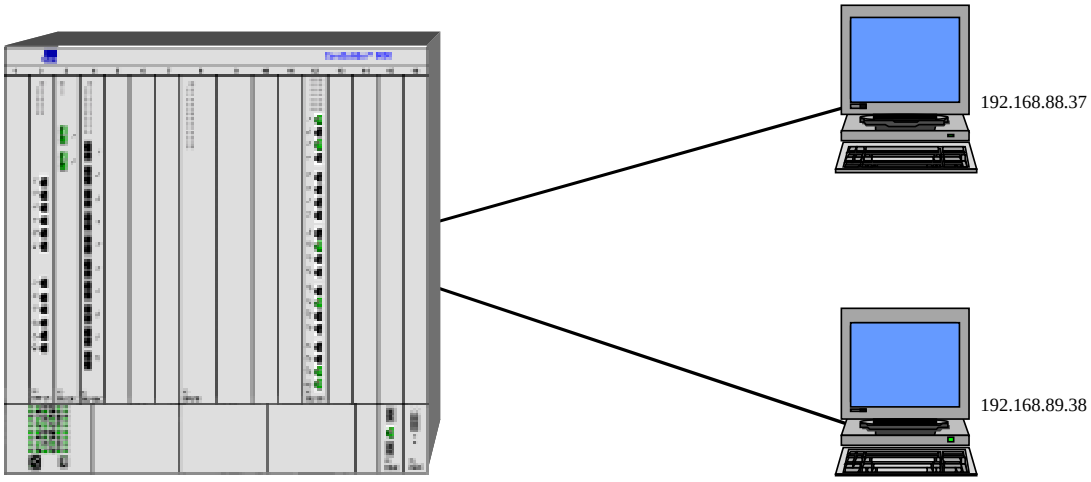

Abb. 20: Testanordnung Layer-3-Switching

4.3.2.2.1 3Com CoreBuilder 9000

Beim CoreBuilder 9000 wurde der *Layer*-3-Durchsatztest durchgeführt, indem jede der beiden Workstations in einem eigenen VLAN an je einem *Port* des 2-*Port*-Gigabit-Ethernet-Moduls angeschlossen wurde und gleichzeitig diese VLANs über den lediglich über 1 GBit/s Bandbreite verfügenden *Backplane Port* in das *Layer*-3-Modul geführt wurden, das in jedem VLAN ein IP-Interface besaß.

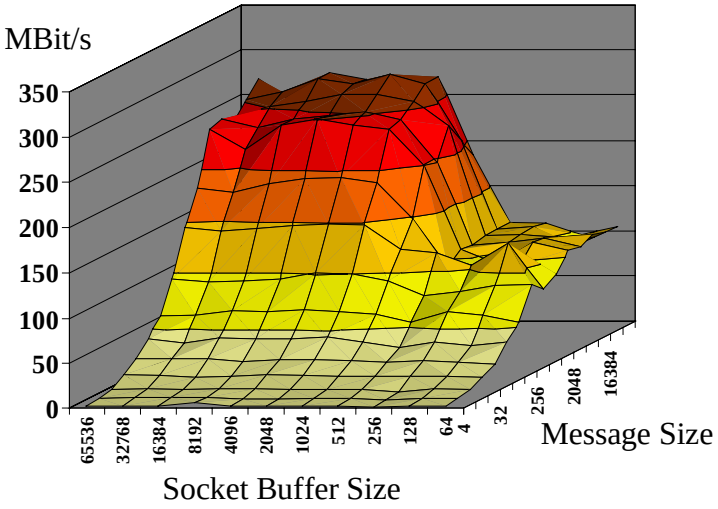

Abb. 21: Ergebnis Netperf Layer 3 mit 3Com CoreBuilder 9000

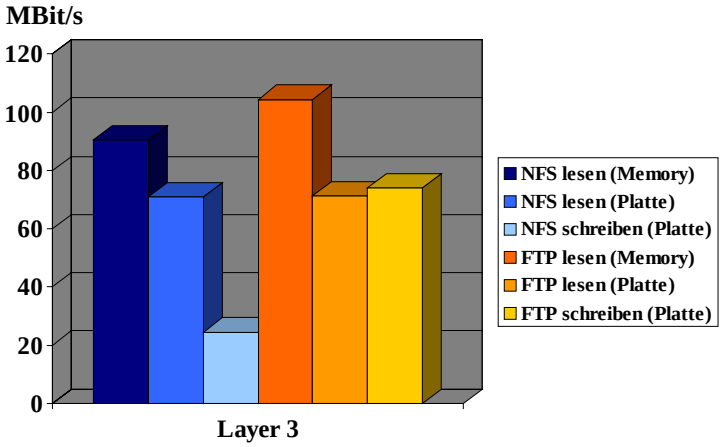

Abb. 22: Ergebnis NFS und FTP Layer 3 mit 3Com CoreBuilder 9000

4.3.2.2.2 Cisco Catalyst 6500

Beim Catalyst 6500 wurden für die teilnehmenden Workstations die gleichen Gigabit-Ethernet-*Ports* wie beim *Layer*-2-Test benutzt, allerdings diesmal in unterschiedlichen VLANs. Beim Router-Modul wurden die vier Gigabit-*Backplane-Ports* zu einem *Channel* zusammengeschaltet und je ein IP-Interface in den betreffenden VLANs eingerichtet.

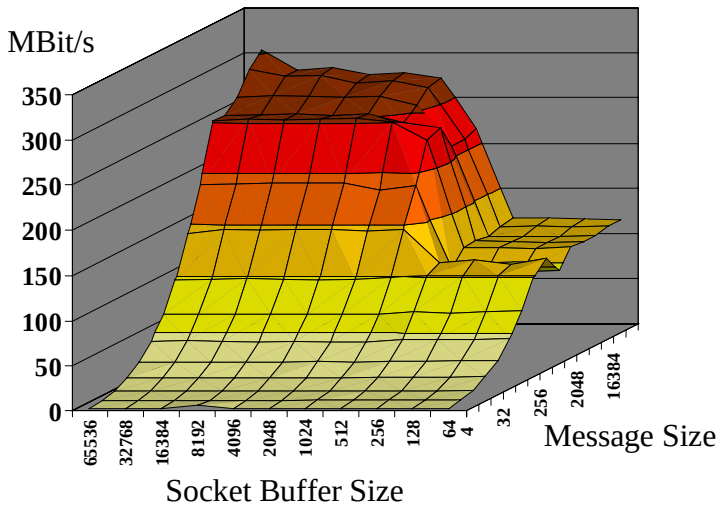

Abb. 23: Ergebnis Netperf Layer 3 mit Cisco Catalyst 6500

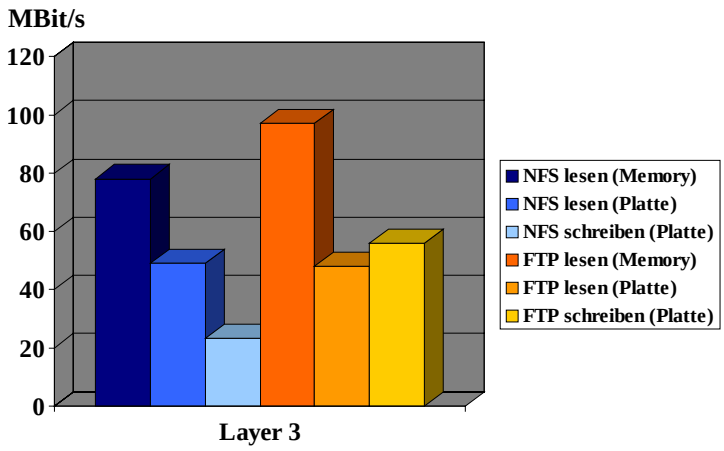

Abb. 24: Ergebnis NFS und FTP Layer 3 mit Cisco Catalyst 6500

4.3.2.2.3 Cabletron SmartSwitch Router 8600

Auch beim *Layer*-3-Durchsatztest unterschieden sich die Ergebnisse von klassischem und *flow-based Switching* nicht.

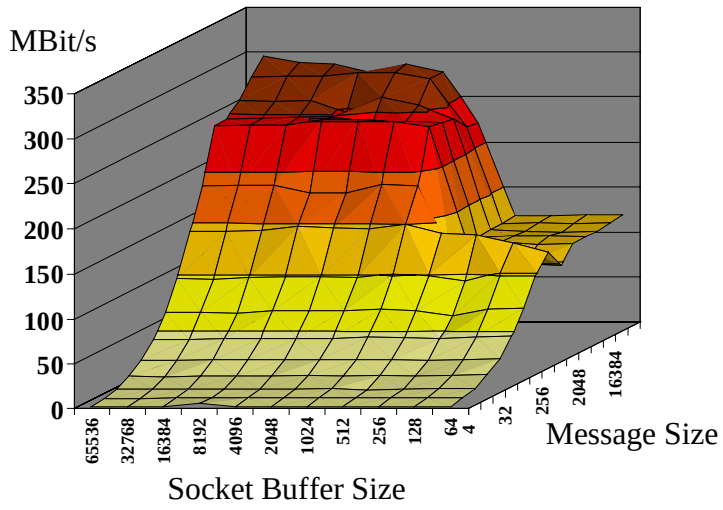

Abb. 25: Ergebnis Netperf Layer 3 mit Cabletron SSR 8600

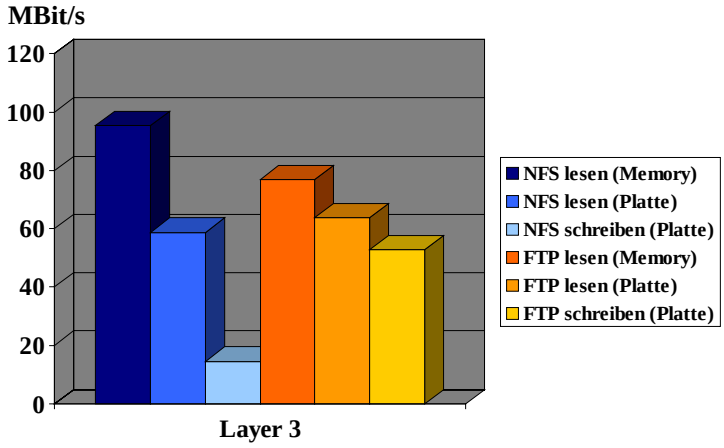

Abb. 26: Ergebnis NFS und FTP Layer 3 mit Cabletron SSR 8600

4.3.3 Konfiguration

Im folgenden werden unter der Überschrift 'Konfiguration' stichpunktartig die Möglichkeiten und Eigenschaften der *Command Line* der jeweiligen *Switches* beleuchtet. Einige der Kategorien stehen natürlich in engem Zusammenhang mit den teilweise in eigenen Kapiteln beschriebenen technischen Fähigkeiten der *Switches*. Die Ausgestaltung des Benutzer-Interfaces und die dort gebotenen Konfigurationsmöglichkeiten sollten im Hinblick auf den Produktionseinsatz bei der Bewertung der *Switches* nicht außer acht gelassen werden.

4.3.3.1 3Com CoreBuilder 9000

– Realisierung des *Command-Line*-Interfaces:

  Hierarchisch; kurze einzeilige Hilfstexte zu den auf der jeweiligen Stufe verfügbaren Befehlen; Befehlsabkürzungen (eindeutiger Teil des Befehles) sind möglich; über mehrere Hierarchiestufen gehende Befehle können komplett in einer Zeile angegeben werden; zur Konfiguration aller Modul-, *Bridge*- oder *Port*-bezogenen Parameter ist die Einwahl auf die Konsole des jeweiligen Moduls notwendig.

– *Scripting* in der *Command Line*:

  Ist nicht implementiert (im Gegensatz z.B. zum wesentlich älteren CoreBuilder-5000-System, das *Scripts* u.a. zeitgesteuert ausführt, und auch im Gegensatz zum CoreBuilder 3500, der den *Layer*-3-Modulen des CoreBuilder 9000 zu Grunde liegt und der die Ausführung von Scripts von einem TFTP-Server anbietet).

– Konfigurationsmanagement:

  Die Modulkonfigurationen liegen als einzelne Files im Filesystem des *Controllers* (*Enterprise Management Engine*, EME); diese Files sind per TFTP bewegbar, aber nicht editierbar (weder lokal noch *remote*); ein ausgetauschtes Modul kann (bei gleichem Modultyp) entweder die Konfiguration des Vorgänger-Moduls oder aber die *Default*-Konfiguration annehmen.

– Softwaremanagement:

  Die Software-*Updates* erfolgen wie auch die Konfiguration modulbezogen, eine neue Modul-Software (*Firmware*) wird per TFTP auf das EME transferiert, von dort kann es auf eines oder mehrere Module eines Typs verteilt werden.

– *Inventory*-Management:

  Über das EME können detaillierte Informationen (Hardware und Software) zu allen Modulen und dem *Environment* (Netzteile, *Powerbudgets*, Temperaturen) angezeigt werden.

– Integrierter Webserver:

  Ist nicht vorhanden.

– *Logging*:

  Das *Logging* für alle Module wird auf dem EME realisiert, die Größe der *Logfiles* sowie ihre Behandlung bei Größenüberschreitung (Stoppen des *Logging* oder FIFO-Behandlung) sowie zeit- und dateigrößengesteuerte Übertragung der *Logfiles* auf einen TFTP-Server sind konfigurierbar. Außerdem werden auf Wunsch SNMP-*Traps* generiert und an eingetragene Server verschickt.

– Sicherheit:

  Im System sind max. zehn Benutzer in drei festen *Access Levels* (*read, write, administer*) mit benutzerabhängigem Password konfigurierbar; von maximal vier gleichzeitigen Telnet-Sitzungen und einem V.24 Zugang darf nur eine Sitzung Administratorrechte besitzen; für den SNMP-Zugang sind maximal zehn *Communities* mit zugehörigen Rechten und jeweils zugeordneter IP-Adresse bzw. IP-Subnetz (mit *Wildcarding*) konfigurierbar.

– DNS-*Support*:

  Ist vorhanden.

– NTP-*Support*:

  Ist nicht vorhanden.

4.3.3.2 3Com SuperStack II 3300 und 3900

– Der 3Com-*Switch* 3300 unterscheidet sich in der Bedienung deutlich vom CoreBuilder 9000. Zwar sind die Befehle ebenfalls hierarchisch mit der Möglichkeit von Abkürzungen und dem Überspringen von Hierarchiestufen organisiert, die Benutzer aber sind in fünf verschiedenen Rechteklassen organisiert, wobei die *Default*-Benutzernamen nicht gelöscht sondern nur um weitere Benutzer ergänzt werden können. Weiterhin sind die *Communities* ähnlich wie Passwörter an die Benutzer gebunden, was die SNMP-Konfiguration nicht vereinfacht und oft zu einer unnötigen Vielzahl von *Community-Strings* führt. Das Management-IP-Interface des *Switches* ist immer mit dem *Default*-VLAN verknüpft, wodurch ebenfalls die Flexibilität im Betrieb des Gerätes leidet. Die Konfiguration ist lediglich im NVRAM gespeichert und nicht transferierbar. Getestet wurde mit der Software Version 2.40, frühere Versionen wie z.B. die Version 2.1 hatten in der *Command Line* nur eingeschränkte Funktionalität (lediglich die IP-Konnektivität des Management-Interfaces konnte konfiguriert werden). Hier sollte der eingebaute Webserver, der jedoch funktional und auch geschwindigkeitsmäßig (Javascript) nicht mit einem *Command-Line*-Interface konkurrieren kann, als primäres Management-Interface dienen.

– Der 3Com-*Switch* 3900 gleicht bezüglich seiner Konfigurationsschnittstelle den *Layer*-2-Modulen des CoreBuilder 9000.

4.3.3.3 Cisco Catalyst 6500

– Realisierung des *Command-Line*-Interfaces:

  Command-Line-Interface in zwei Modi: einfacher Modus lediglich zur Anzeige einiger Informationen (*read-only*), *Enabled*-Modus mit der Möglichkeit, alle Parameter zu ändern (*read/write*); keine Befehlshierarchie; alle Befehle sind direkt in der *Command Line* ausführbar; mit einem Fragezeichen können mögliche Parameter und Schlüsselwörter innerhalb eines Befehls mir kurzen erläuternden Texten aufgelistet werden; Befehlsabkürzungen (eindeutiger Teil des Befehles) sind nur eingeschränkt möglich; eine *Command History* und *Command Editing* können benutzt werden; die Konfiguration der *Layer*-3-Funktionen ist auf der separaten Konsole des *Layer*-3-Tochter-*Boards* des *Supervisor*-Moduls vorzunehmen, zu der man sich von der *Switch*-Konsole aus verbinden kann.

– *Scripting* in der *Command Line*:

  Ist nicht implementiert.

– Konfigurationsmanagement:

  Die Konfiguration des Gesamtsystems und des *Layer*-2-Teils wird getrennt von der Konfiguration des *Layer-3-Boards* (MSM) gehalten; Konfigurationsänderungen am *Switch* werden sofort wirksam, ins NVRAM gespeichert und können jederzeit im Klartext angezeigt und per TFTP in lesbarer Form transferiert werden; die *Layer*-3-Konfigurationen werden, wie beim Cisco IOS üblich, in Form einer aktiven Konfiguration und einer beim Neustart aktivierten Startkonfiguration gehalten; auch die Router-Konfiguration kann als lesbares File über TFTP gesichert und auch wieder eingespielt werden.

– Softwaremanagement:

  Neue Software des *Switches* wird per TFTP ins *Flash Memory* transferiert, wobei der *Switch* und die *Layer*-3-Karte getrennte Software-*Images* benutzen; über einen Befehl wird das zu benutzende Software-*Image* festgelegt und durch einen Neustart aktiviert.

– *Inventory*-Management:

  Über die Konsole können detaillierte Informationen (Hardware und Software) zu allen Modulen und dem *Environment* (Netzteile, *Powerbudgets*, Temperaturen) angezeigt werden.

– Integrierter Webserver:

  Ist nicht vorhanden.

– *Logging*:

  Verschiedene *Logs* (*boot log* und normaler *event log* für alle Module) in Puffern auf dem System und über den üblichen *Syslog*-Dienst an *Log*-Server weiterleitbar; SNMP-*Traps* werden ebenfalls unterstützt.

– Sicherheit:

  Im *Switch* werden zwei Passwörter verschlüsselt gehalten. Das eine ermöglicht nur einen lesenden Zugriff über das CLI auf das System, während mit dem zweiten Passwort auch ein schreibender Zugriff ermöglicht wird; alternativ ermöglicht der *Switch* den Einsatz eines TACACS-Servers zur Validierung von Benutzern; für jede der drei SNMP-Zugriffsrechte *read-only*, *read/write* und *read/write all* ist jeweils nur ein *Community String* konfigurierbar; weiterhin kann der Zugriff auf das System über Telnet und SNMP anhand einer *Access*-Liste mit Netzmasken auf IP-Netze oder auch einzelne IP-Adressen eingeschränkt werden.

– DNS-*Support*:

  Ist vorhanden.

– NTP-*Support*:

  Ist vorhanden.

4.3.3.4 Cisco Catalyst 2948G

– Das Management-Interface des Catalyst 2948G ähnelt stark dem des Catalyst 6500. Die Handhabung der *Command Line*, der Software-*Upgrade*, die Konfigurationsverwaltung in Dateiform, die IP- und SNMP-Konfiguration und auch die Sicherheitsmöglichkeiten (IP-*Access*-Einschränkungen) sind identisch. Abweichungen gibt es lediglich bei der Aktivierung und Konfiguration einiger weniger *Features*, über die der 2948G im Vergleich zur 6000er Familie nicht verfügt (wie z.B. der Einschränkung des *Broadcast*-Anteils im Verkehr).

4.3.3.5 Cabletron SmartSwitch Router 8600

– Realisierung des *Command-Line*-Interfaces:

  Command-Line-Interface (CLI) in drei Modi: *User Mode* lediglich zur Anzeige einiger Informationen (*read-only*), *Enable*-Modus mit umfassenden Informationen und Statistiken, *Config*-Modus zur Konfiguration in einen Zwischenspeicher (*scratchpad*) und anschließender Aktivierung der gesammelten Änderungen; eine *Command History* und *Command Editing* können benutzt werden; alle Parameter (incl. *Layer*-3-Konfiguration) können von einem CLI aus ausgeführt werden.

– *Scripting* in der *Command Line*:

  Ist nicht implementiert.

– Konfigurationsmanagement:

  Die Konfigurationen liegen als *Scratchpad* (noch nicht aktiv), *Active* (Produktion) und *Startup* (Aktivierung nach dem Neustart) auf den *Control*-Modulen bzw. deren *Flash Cards* in einem Filesystem vor, sie sind als Klartext einsehbar und können mit TFTP bewegt werden (*up*- und *download*).

– Softwaremanagement:

  Eine neue Softwareversion kann über TFTP auf den *Switch* geladen werden (der Transfer dauert ca. 5 Sekunden, das anschließende Auspacken des komprimierten *Image* ca. 25 Minuten (ohne Störung der Produktion)), anschließend wird das zu benutzende *Image* festgelegt und der *Switch* neu gestartet.

– *Inventory*-Management:

  Über die Konsole können Informationen (Hardware und Software) zu allen Modulen und Statusangaben zu den Netzteilen und Lüftern angezeigt werden.

– Integrierter Webserver:

  Ist nicht vorhanden.

– *Logging*:

  Der *Switch* unterstützt den üblichen *Syslog*-Dienst zur Weiterleitung von Ereignissen verschiedener Kategorien an *Log*-Server; SNMP-*Traps* werden ebenfalls unterstützt.

– Sicherheit:

  Die oben erwähnten *User*-Modi sind durch Passwörter abgesichert; die Passwörter werden verschlüsselt in der Konfiguration abgelegt; alternativ kann auch ein externer TACACS-, TACACS+- oder RADIUS-Server zur Benutzervalidierung genutzt werden; SNMP-*Communities* können für *Read-only*- und *Read/write*-Zugriff gesetzt werden; weitere Zugriffseinschränkungen zum Management-Interface können durch die im System definierbaren *Access Control Lists* (ACLs) realisiert werden.

– DNS-*Support*:

  Ist vorhanden.

– NTP-*Support*:

  Ist vorhanden.

4.3.3.6 SmartSwitch 2200 und SmartStack ELS100 24TXG

– Bei beiden *Switches* war das Benutzerinterface nicht als *Command Line* im klassischen Sinne, sondern als ein auf Eingabemasken basierendes *Full-Screen*-Menü realisiert. Die Konfiguration von Parametern ist nur im entsprechenden Menü und an der entsprechenden Stelle im Menü möglich. Ein Überspringen von Menüebenen oder Abkürzen von Befehlen ist nicht möglich. Erschwerend kommt hinzu, daß logisch zusammengehörende und oftmals gleichzeitig zu ändernde Parameter über mehrere Menüebenen und –zweige verteilt und teilweise nicht eindeutig bezeichnet sind. Auffällig war u.a., daß bei jeder Änderung der IP-Adresse des *Switches* dieser ein *Reset* durchführte, daß pro SNMP-Zugriffsrecht (*read-only, read/write*) nur eine *Community* konfiguriert werden konnte und daß diese *Community* gleichzeitig das Password für den Konsolzugang (Telnet oder V.24) darstellte.

4.3.4 RMON Implementierung

Die getesteten *Switches* hatten allesamt nur eine sehr rudimentäre RMON-Unterstützung. Implementiert war auf den *Switches* trotz teilweise weitergehender Angaben in den Datenblättern der Hersteller lediglich mini-RMON mit den Gruppen *Statistics, Alarms, Events*. Weitere Gruppen oder gar RMON2 standen selbst auf den intelligenteren Modulen wie dem *Layer*-3-Modul des CoreBuilder 9000 nicht zur Verfügung.

Lediglich die kleinen *Switches* 3300 und 3900 von 3Com gestatteten bei allerdings eingeschränkter Speicherausstattung innerhalb dieser Grenzen auch die Nutzung von *Host*-basierenden RMON-Gruppen. Getestet wurde mit der LANsentry-Software aus der 3Com *Transcend Management Suite* sowie dem Netscout-Manager der Firma Frontier Software.

Als Alternative zum Analysieren des Internverkehrs bieten alle *Switches* die Möglichkeit, Verkehr von einem *Port* auf einen Analyse-*Port* zu spiegeln, an den typischerweise eine vollwertige RMON-*Probe* oder ein Netzwerkanalysator angeschlossen ist. Dieses *Port*-SPAN genannte Verfahren unterliegt je nach Hersteller und *Switch* einigen Einschränkungen. Neben den offensichtlichen Einschränkungen, wie einem passenden Bandbreitenverhältnis von *Source-Port* zu Analyse-*Port* von mindestens 1:1, gibt es Einschränkungen bezüglich der maximalen Anzahl gleichzeitiger solcher SPAN-Sessions, bezüglich der Lokalität von *Source*- und Analyse-*Port* (die z.B. auf einem Modul liegen müssen) oder auch bezüglich zusätzlicher Eigenschaften des *Source-Port* (*Trunk, Channel*). Besonders auffällig war diesbezüglich die Einschränkung des SSR 8600, daß das gesamte Modul, auf dem der Analyse-*Port* liegt, nicht mehr für normales *Switching* genutzt werden kann und somit immer unbeschaltet bleiben sollte.

4.3.5 Fehler

Im folgenden werden einige der wichtigeren Fehler aufgelistet, die während der Tests entdeckt wurden:

- Der bei den DEC-Workstations verwendete Gigabit-Ethernet-Adapter war, in Kombination mit dem verwendeten OS-*Release*, nicht in der Lage, UDP-Verkehr zu führen. Wurden UDP-Verbindungen aufgebaut, so reduzierte sich der erreichbare Durchsatz innerhalb weniger Sekunden auf wenige KBit/s, teilweise wurden davon auch andere Interfaces (z.B. das eingebaute Fast-Ethernet-Interface) in Mitleidenschaft gezogen. Die betroffenen Workstations konnten erst nach einem Neustart wieder normal im Netzwerk arbeiten. Der Fehler trat u.a. bei UDP-basiertem NFS oder auch bei TFTP auf.
- In einer Testkonfiguration nach Abb. 18 auf Seite 32 (ohne Priorisierung) mit zwei Cisco-*Switches* wurden lediglich Durchsätze von ca. 15 MBit/s zwischen zwei Gigabit-Ethernet-Teilnehmern über eine Fast-Ethernet-Strecke zwischen den *Switches* erreicht. Die Ergebnisse waren jederzeit wiederholbar. In gleicher Konfiguration arbeiteten z.B. zwei 3Com-*Switches* mit ca. 95 MBit/s Durchsatz. Nach einem Software-*Upgrade* des Catalyst 2948G von Version 5.2.1 auf Version 5.2.2 konnte das Verhalten nicht mehr beobachtet werden. Es wurden, wie bei den anderen Herstellern auch, über 90 MBit/s Durchsatz gemessen.

– Der beim 3Com CoreBuilder konfigurierbare und vom Hersteller schon fast empfohlene *Switching*-Modus *'all open'*, bei dem pro *Switch* (Modul) für alle VLANs eine gemeinsame *Forwarding Database* benutzt wird, kann in einigen Netzwerkkonfigurationen logischerweise zu Problemen führen. Dazu zählt z.B. eine Konfiguration, in der zwei Interfaces eines Netzwerkteilnehmers in unterschiedlichen VLANs mit unterschiedlichen IP-Adressen gleiche MAC-Adressen benutzen.

  Ein Beispiel dazu wäre eine Sun-Workstation, die als *Default*-Einstellung für alle ihre Netzwerkinterfaces die gleiche MAC-Adresse benutzt. Würden Pakete dieser Interfaces, in getrennten VLANs (IP-Netzen) über ein Modul geführt, so würde zu jedem Zeitpunkt nur ein *Port*-Eintrag zu dieser MAC-Adresse in der *Forwarding Database* existieren und für diese Workstation bestimmte Pakete nahezu zufällig auf einen der beiden zu der Workstation führenden *Ports*, teilweise mit VLAN-Übergang, weitergeleitet. Das gleiche gilt bei (vorsätzlicher) Konfiguration einer falschen MAC-Adresse (verbunden mit einer falschen IP-Konfiguration). In diesem Fall könnte ebenfalls Verkehr die VLAN-Grenzen, die ja auch Sicherheitsgrenzen sein können, ohne einen Router und evtl. dort konfigurierte ACLs zu durchlaufen, überwinden. Verifiziert wurde dies durch folgende Konfiguration:

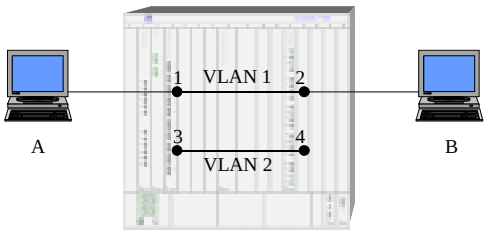

Abb. 27

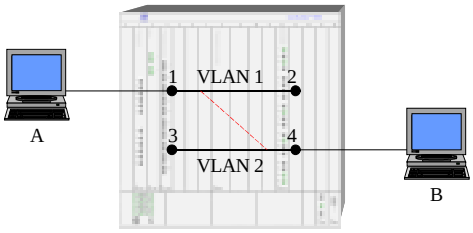

Abb. 28

In einem CoreBuilder 9000 im *All-Open*-Modus wurden zwei VLANs konfiguriert, zwischen denen nicht geroutet wurde. Die *Ports* 1 und 2 wurden dem VLAN 1, die *Ports* 3 und 4 dem VLAN 2 zugeordnet. An die *Ports* 1 und 2 wurden die Workstations A und B mit IP-Adressen innerhalb eines Subnetzes angeschlossen und zwischen ihnen kommuniziert (Abb. 27). Während dieser Kommunikation wurde die Workstation B von *Port* 2 auf *Port* 4 umgesteckt. Nach wenigen Sekunden (*Port* 4 mußte den *Spanning Tree Forwarding Status* erreichen und die Workstation B ein zufälliges Paket verschicken, mit dem die *Forwarding Database* des *Switches* aktualisiert wurde) wurde die Kommunikation fortgesetzt, obwohl die Teilnehmer komplett getrennten VLANs zugeordnet waren (Abb. 28). Die Tatsache, daß für den Teilnehmer B im ARP-*Cache* des Teilnehmers A noch ein Eintrag vorhanden war, kombiniert mit der gemeinsamen *Forwarding Database* aller VLANs im *Switch* im Modus *'all open'*, ermöglichte dieses Verhalten.

An dieser Stelle sei noch einmal vor den Risiken von VLAN-Implementierungen mit gemeinsamer *Forwarding Database*, die VLANs lediglich als Container für

Broadcasts realisieren, *Unicasts* aber zwischen VLANs weiterleiten, mit all ihren Risiken im Netzwerkbetrieb gewarnt.

– Ein ähnliches Problem wie beim CoreBuilder 9000 im *All-Open*-Modus wurde auch beim Cabletron SSR 8600 gesehen. Hier wurde beim *Flow Based Switching* ein eingerichteter und aktiver *Flow* (siehe Abb. 29) nicht beendet, wenn einer der beteiligten *Ports* in ein anderes VLAN konfiguriert wurde (Abb. 30). Die kommunizierenden Maschinen konnten über die bereits in Benutzung befindlichen TCP-*Ports* weiter kommunizieren (teilweise tagelang). Ein neuer *Flow* (gleiche Maschinen, anderer TCP-*Port*) konnte nicht aufgebaut werden. Dieser Fehler wurde an Cabletron gemeldet.

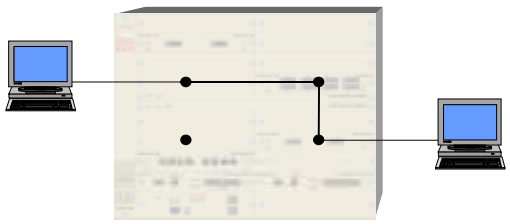

Abb. 29

Abb. 30

5 Zusammenfassung / Bewertung

Die Tests haben gezeigt, daß die *Switches* der verschiedenen Hersteller sich weniger in den im Rahmen dieses Tests untersuchten Durchsatzleistungen, als vielmehr in vielen Punkten, wie z.B. der Realisierung von VLANs, dem *Layer-3-Switching*, dem Priorisieren von Verkehr oder auch den Managementschnittstellen unterscheiden.

Diese Unterschiede sind teilweise durch verschiedene Philosophien der Hersteller begründet, spiegeln aber auch deutlich die Historie der jeweiligen Firma wider.

Insbesondere bei den kleineren *Switches* scheinen viele *Features* wie z.B. das VLAN-*Tagging* nachträglich implementiert worden zu sein und sind teilweise nur mit erheblichen Einschränkungen zu nutzen.

Ebenfalls sichtbar ist die Aquisitionshistorie vieler Firmen. So haben z.B. die 3Com-*Switches* SuperStackII 3300 und 3900 trotz sehr ähnlicher Ausstattung und eines bis auf einige Details vergleichbaren Einsatzprofils aufgrund getrennter Entwicklerteams (teilweise Mitarbeiter aus der Chipcom-Übernahme) sehr unterschiedliche Benutzerschnittstellen (*Command Line Interface*) und ähneln sich in dieser Hinsicht nicht mehr als *Switches* verschiedener Hersteller. Ähnliches kann auch zu den Unterschieden zwischen dem Cabletron SmartSwitch Router 8600 und den *Access-Switches* SmartSwitch 2200 und SmartStack ELS100 gesagt werden.

Die sich in vielen Punkten stark gleichenden Broschüren und Produktbeschreibungen der getesteten Hersteller zu ihren großen und kleinen *Switches* wurden jedenfalls nach dem Test mit anderen Augen gelesen; der eine oder andere Konjunktiv fiel erst nach den Tests als solcher auf.

Für den Betrieb eines Campus-LAN mit ca. 6.000 Endgeräten und wachsenden Anforderungen in puncto Bandbreite, Sicherheit und verzögerungsfreiem Transport von *Content Streams* (Video, Telefonie) ist jedoch die konsequente und kompromißlose Umsetzung aktueller Standards, verbunden mit effektiven Managementmöglichkeiten der Komponenten, eine wesentliche Voraussetzung.

Während die Firma 3Com im Bereich des *Layer-2-Switching* bereits viele Jahre Erfahrung hat und dies teilweise in den getesteten Komponenten zu spüren ist, führte die Realisierung des *Layer-3-Switching* im CoreBuilder 9000, die nicht einmal eine 1:1 Übernahme des z.Zt. im Forschungszentrum Jülich mit Cisco-7000-Routern realisierten *Layer*-3-Netzübergangs aufgrund der fehlenden *Secondary* IP-Adressen erlaubt hätte, dazu, daß die 3Com *Switch*-Familie als nicht geeignete Plattform für die Kommunikation des Forschungszentrums in den nächsten Jahren angesehen wurde. Ebenfalls enttäuschend waren hier die großen funktionalen Einschränkungen bei der Wahl des sicheren, auf getrennten MAC-Tabellen beruhenden *all closed Switching*-Modus, sowie die Einschränkungen beim *Trunking* (Gigabit-Module zählen als *Trunk* für die *Backplane*, nach jeder *Trunk*-Definition muß der *Switch* neu gestartet werden).

Bei den Produkten der Firma Cisco, bei der die kleinen und großen *Switches* eine fast identische Benutzerschnittstelle aufwiesen, störte die beim *Access Switch* nicht mögliche Begrenzung des *Broadcast*-Anteils des Verkehrs und die noch sehr eingeschränkte Funktionalität (kein IOS) der Router-Implementierung per MSM (*Multilayer Switch Module*). Hier war jedoch das Nachfolgeprodukt MSFC (*Multilayer Switch Feature Card*) bereits angekündigt, das mit Cisco IOS gefahren wird und eine Vielzahl der auch auf den eigenständigen Routern verfügbaren Merkmale aufweist. Aus Sicht des Netzwerkpraktikers fehlt bei den Cisco-*Switches* auch ein wenig die Signalisierung der Auslastung einzelner *Ports* über LEDs am Gerät, wie sie bei 3Com und Cabletron anzutreffen ist. Die VLAN-Implementierung mit komplett getrennten Adreßtabellen sowohl bei dem kleinen als auch dem großen *Switch* und auch die Flexibilität beim Einsatz von *Trunking* und *Channeling* sowie die Ausrichtung auf zukünftig wichtige Themen wie z.B. QoS/Priorisierung, *Multicast*-Verkehrsführung, ACLs (*Access Control Lists*) und dem *Accounting* auf Basis von *Layer*-3- und *Layer*-4-Informationen lassen die Catalyst *Switches* als interessante Kandidaten für einen Einsatz im JuNet erscheinen.

Die *Switches* der Fa. Cabletron wiesen eine sehr unterschiedliche Konfigurationsoberfläche auf. Während der SmartSwitch Router 8600 zeitgemäß mit einer *Command Line* arbeitete, ließen sich die *Switches* SmartSwitch 2200 und SmartStack ELS100 nur über Bildschirmmasken (*full screen*) mit festen Eingabefeldern konfigurieren, bei denen logisch zusammgehörende Parameter teilweise über mehrere Hierarchiestufen hinweg getrennt anzugeben waren. Hier soll der SmartSwitch 6000, der jedoch beim Test nicht zur Verfügung stand, besser zu bedienen sein. Der SSR 8600 hatte zum Zeitpunkt des Tests die umfangreichsten Möglichkeiten im *Layer*-3-Bereich, die z.B.

auch die Erstellung von ACLs beinhalteten. Auch das *Switching* auf der Basis von *Flows* (MAC- und IP-Adressen sowie *Layer-4-Port*-Nummern) für alle *Ports* des *Switches* mit den zugehörigen Optionen, wie z.B. *flow*-basiertes *Accounting*, sind durchaus zukunftsweisende Konzepte. Nicht ausreichend für die avisierten Einsatzbereiche war jedoch die *Port*-Dichte des Gerätes. Hier sollen neue Module, teilweise mit MT-RJ-Steckungen, erscheinen.

Generell muß gesagt werden, daß sich der Aufwand des Tests der verschiedenen *Switches* gelohnt hat. Die Unterschiede in der Implementierung diverser Techniken sind erheblich, und es kann jedem, der vor einer ähnlichen Entscheidung steht, geraten werden, ebenfalls zu testen oder aber zumindest nach den Hochglanzprospekten der Hersteller auch die *Implementation Guides* und *Command References* kritisch zu lesen, in denen so manche Offenbarung auf ihre Entdeckung wartet.

6 Literatur

[1] 3Com: CoreBuilder 9000: Implementation Guide, Release 2.1.0.

[2] 3Com: Super Stack II Switch 3300: User Guide.

[3] 3Com: Super Stack II Switch 3900 and Switch 9300: Administration Guide.

[4] 3Com: Super Stack II: Switch Management Guide.

[5] 3Com: CoreBuilder 3500: Implementation Guide.

[6] 3Com: CoreBuilder 9000: Administration Console User Guide.

[7] 3Com: CoreBuilder 9000: Command Reference Guide.

[8] Cabletron: SmartStack 100 ELS100-24TXG Ethernet Switch: Installation and User Guide.

[9] Cabletron: SmartSwitch 2200: User's Guide.

[10] Cabletron: SmartSwitch Router 8000/8600: Getting Started Guide.

[11] Cabletron: SmartSwitch Router: Command Line Interface Reference Manual.

[12] Cisco: Catalyst 6000 and 6500 Series: Command Reference (5.1).

[13] Cisco: Catalyst 6000 and 6500 Series: Multilayer Switch Module Installation and Configuration Note.

[14] Cisco: Catalyst 6000 and 6500 Series: Software Configuration Guide (5.1).

[15] Cisco: Catalyst 5000 family, 4000 family and 2948G Switches: Command Reference (5.2).

[16] Cisco: Catalyst 5000 family, 4000 family and 2948G Switches: Software Configuration Guide (5.2).

[17] Köhler, R.-D., Kemmler, W.: Gigabit - Ethernet, 3Com – die Komponenten der Zukunft. Fossil Verlag, Köln, 1998, ISBN 3-931959-21-X.

[18] Mextorf, O.: Technik und Einsatzmöglichkeiten von Fast Ethernet im Forschungszentrum Jülich. FZJ-ZAM-IB-9817, 1998.